Annals of Pure and Applied Logic 58 (1992) 29–55
North-Holland

A transfer theorem in constructive p-adic algebra*

Deirdre Haskell

School of Mathematical Sciences, Queen Mary and Westfield College, Mile End Road, London, United Kingdom E1 4NS

Communicated by A. Nerode
Received 1 November 1990
Revised 16 November 1991

Abstract

Haskell, D., A transfer theorem in constructive p-adic algebra, Annals of Pure and Applied Logic 58 (1992) 29–55.

The main result of this paper is a transfer theorem which describes the relationship between constructive validity and classical validity for a class of first-order sentences over the p-adics. The proof of one direction of the theorem uses a principle of intuitionism; the proof of the other direction is classically valid. Constructive verifications of known properties of the p-adics are indicated. In particular, the existence of cylindric algebraic decompositions for the p-adics is used.

1. Introduction

This paper is concerned with the constructive theory of the p-adic numbers. In particular, it studies the relationship between constructive validity and classical validity for first-order sentences over the p-adics. This relationship is elucidated by the 'transfer theorem' which is the main result of this paper. By 'constructive' I am referring to constructive mathematics in the style of Bishop [2], in which real or p-adic numbers are Cauchy sequences of rationals convergent at a predetermined rate, in the real or p-adic metric, respectively. The Bishop school is consistent with both classical and intuitionistic mathematics. Background for the reader can be found in [1, 3, 14]. The latter reference is particularly relevant to Section 2.

Correspondence to: Dr. D. Haskell, Department of Mathematics, College of the Holy Cross, Worcester, MA 01610-2395, United States.

* This research was partly supported by graduate research assistantships at Stanford University and an SERC post-doctoral research assistantship at Queen Mary and Westfield College of the University of London.

In [19], Scowcroft proves a transfer theorem which describes the relationship between constructive and classical validity for a class of real algebraic sentences. This paper extends his methods to an analogously defined class of p-adic algebraic sentences.

The transfer theorem applies to a class of sentences built from simple formulae (these are defined in Section 2). Given any simple formulae $M(\boldsymbol{x})$ in m variables and $N(\boldsymbol{x}, \boldsymbol{y})$ in $m+n$ variables, a method is given in Lemma 3.2 for constructing a third formula $G(\boldsymbol{x}, \boldsymbol{y})$ from M and N. Informally, G says that the tuples $\boldsymbol{y}$ for which $N(\boldsymbol{x}, \boldsymbol{y})$ holds depend continuously on the tuples $\boldsymbol{x}$ for which $M(\boldsymbol{x})$ holds. The first direction of the transfer theorem can be stated as follows.

Theorem A. $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$ *holds constructively if*

$$\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$$

holds classically.

That is, for this class of sentences it suffices to prove the classical theorem with G in order to prove the constructive theorem with N. This is proved in Section 3 (Theorem 3.4) and is analogous to [19, Theorem 1]. The other direction of the transfer theorem suggests a limitation to what can be proved constructively. It has a principle of intuitionism as hypothesis; this is explained in more detail in Section 4.

Theorem B. *Assume Brouwer's principle for numbers.* $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$ *holds classically if* $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$ *holds constructively.*

That is, the constructive validity of the sentence with N implies a continuity property classically. This is proved in Section 4 (Theorem 4.3) and is analogous to [19, Theorem 2].

Throughout this paper I will be working constructively. Thus, when I say that a formula is valid or holds without a qualifier, I will always mean constructively valid or holds constructively. In order for Theorems A and B to be constructive theorems, we need to have a way of considering 'classical validity' from a constructive standpoint. For both the reals and the p-adics, this is provided by the algebraic numbers. The set of algebraic p-adics Q_p is a field inside the ring of constructive p-adics $\mathbb{Q}_p$, and the constructive first-order theory of Q_p is the classical first-order theory of p-adically closed fields. Similarly, the set of algebraic reals R is a field in $\mathbb{R}$, and the constructive first-order theory of R is the classical theory of real closed fields. Axiomatic and algebraic properties of Q_p and $\mathbb{Q}_p$ are described in Section 2.

A discussion of a simple example of the first direction of the transfer theorem provides some insight into the proof in the general case. Consider the problem of solving a system of linear equations in n variables, $X\boldsymbol{y} = \mathbf{1}$, where $\mathbf{1}$ is the vector of length n with 1 for each coefficient. The coefficients of the matrix X are given

by points $\boldsymbol{x} \in \mathbb{Q}_p^{n^2}$ (or $\mathbb{R}^{n^2}$). The sentence

$$\forall \boldsymbol{x}\,(\det(X) \neq 0 \rightarrow \exists \boldsymbol{y}\,(X\boldsymbol{y} = \mathbf{1})) \qquad (*)$$

holds classically. In order to prove (*) constructively, fix a point $\boldsymbol{x} \in \mathbb{Q}_p^{n^2}$ (respectively $\mathbb{R}^{n^2}$) at which $\det(X) \neq 0$. $\boldsymbol{x}$ is given by a Cauchy sequence of rational points $(\boldsymbol{x}_n)$ which converges at the rate $|\boldsymbol{x}_k - \boldsymbol{x}_l| \leq p^{-\min\{k,l\}}$ for every $k, l \geq 1$ (in $\mathbb{R}$, $|\boldsymbol{x}_k - \boldsymbol{x}_l| \leq k^{-1} + l^{-1}$), and the inequality $\det(X) \neq 0$ includes the information that $\det(X)$ is bounded away from zero. (The precise, constructive definitions are given in Section 2.) One must construct a Cauchy sequence $(\boldsymbol{y}_k)$ satisfying the same rate-of-convergence condition in order to obtain a p-adic point $\boldsymbol{y}$ for which $X\boldsymbol{y} = \mathbf{1}$. The $\boldsymbol{y}_k$ need not be rational points, but they must be determined by a finite amount of information about $\boldsymbol{x}$. Thus, one must generate a subsequence $(\boldsymbol{x}_{n_k})$ of $\boldsymbol{x}$ and associate with each $\boldsymbol{x}_{n_k}$ a $\boldsymbol{y}_k$ so that the sequence $(\boldsymbol{y}_k)$ converges and satisfies $X_{n_k}\boldsymbol{y}_k = \mathbf{1}$.

Let X_k be the matrix with coefficients $\boldsymbol{x}_k$. In order to use the classically true sentence (*), the sequence $(\boldsymbol{x}_k)$ should satisfy $\det(X_k) \neq 0$ for every k. One can then use Cramer's rule to write explicitly a continuous, vector-valued function f such that $\boldsymbol{y} = f(\boldsymbol{x}_k)$ is the solution to the equation $X_k\boldsymbol{y} = \mathbf{1}$. This further information about the continuous dependence of $\boldsymbol{y}$ on $\boldsymbol{x}$ is what is required for the predicate G. (In general, G will not define a single-valued function.) It is now natural to take $\boldsymbol{y}_1 = f(\boldsymbol{x}_1)$, but this choice may not be the correct one. The rate of convergence required for the $(\boldsymbol{y}_k)$ is that $|\boldsymbol{y}_1 - \boldsymbol{y}_k| \leq p^{-1}$ (respectively ≤ 1) for every $k > 1$. Since f is continuous, there will be a $\delta \neq 0$ so that, if $|\boldsymbol{x}_1 - \boldsymbol{x}_k| < |\delta|$, then $|f(\boldsymbol{x}_1) - f(\boldsymbol{x}_k)| \leq p^{-1}$ (respectively ≤ 1), but there is no guarantee that there is an $\boldsymbol{x}_k$ within distance $|\delta|$ of $\boldsymbol{x}_1$, leaving no obvious way to choose $\boldsymbol{y}_2$. One needs to use the stronger fact that f is uniformly continuous on sets of the form $B = \{\boldsymbol{z} \in \mathbb{Q}_p^{n^2} : |\det(Z)| \geq p^{-b_1} \,\&\, |\boldsymbol{z}| \leq p^{-b_2}\}$, where $b_1, b_2 \in \mathbb{Z}$. The constructive reading of $\det X \neq 0$ allows one to suppose there is a uniform lower bound on $|\det(X_k)|$. Hence one can find a set B containing $\boldsymbol{x}$ and the sequence $(\boldsymbol{x}_k)$ on which f is uniformly continuous. So there is a $\delta \neq 0$ such that, for any k, l, if $|\boldsymbol{x}_k - \boldsymbol{x}_l| < |\delta|$, then $|f(\boldsymbol{x}_k) - f(\boldsymbol{x}_l)| < p^{-1}$ (respectively > 1). Now we can let $\boldsymbol{y}_1 = f(\boldsymbol{x}_{n_1})$, where n_1 is an integer large enough so that $p^{-n_1} < |\delta|$ (respectively $n_1^{-1} < |\delta|$). For then every $\boldsymbol{x}_n$ with $n \geq n_1$ is within $|\delta|$ of $\boldsymbol{x}_{n_1}$, and thus there are possible choices for the next elements of the sequence. To conclude, one remarks that, since $X_{n_k}\boldsymbol{y}_k = \mathbf{1}$ for every k, this equality also holds in the limit.

The difficulties that arise in the general case, as compared with this example, deserve some comment. In general, one supposes that $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$ holds over Q_p. To establish that $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$ holds over $\mathbb{Q}_p$, one is presented with $\boldsymbol{x} \in \mathbb{Q}_p^m$ such that $M(\boldsymbol{x})$ holds, and one has to find $\boldsymbol{y} \in \mathbb{Q}_p^n$ such that $N(\boldsymbol{x}, \boldsymbol{y})$ holds. In order to make use of the assumption, one must have a sequence $(\boldsymbol{x}_k)$ from Q_p^m converging to $\boldsymbol{x}$ such that $M(\boldsymbol{x}_k)$ holds for each k. On the other side of the implication, if N does not define a closed set, one must choose the points $(\boldsymbol{x}_k, \boldsymbol{y}_k)$ obeying G with care to ensure that N holds in the limit. That both of

these can be done when M and N are simple formulae is shown by the crucial Lemma 3.1, which uses the geometry of cylindrical algebraic decompositions to show that a constructive number (real or p-adic) can be approximated by a sequence of algebraic numbers with special properties.

The other major difficulty in the general case comes in the adaptation of familiar compactness arguments to obtain uniform versions of the continuity property of G over closed and bounded subsets. These arguments are not, in general, constructively valid. However, it turns out that they are only needed over the algebraic numbers, where, as is shown in Section 2, they can be constructively justified.

The continuity property of G tells us that the other direction of the transfer theorem is not true if interpreted classically. If $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$ holds classically, it does not necessarily follow that $\boldsymbol{y}$ depends continuously on $\boldsymbol{x}$. So the proof of this direction must require the use of some nonclassical principle, and it is natural to turn to intuitionism. Scowcroft [19] has shown that Brouwer's principle for numbers [5] implies a weak form of Brouwer's principle for functions, and it is the latter which is employed in the proof of Theorem 4.3. The difficulty comes in trying to apply the principle, which is stated in terms of functions on Baire space, in this new context. The application requires the existence of continuous functions mapping Baire space onto certain specially defined subsets of $\mathbb{Q}_p^n$ (respectively $\mathbb{R}^n$). The construction of these functions, which is highly technical, is given in Lemma 4.2. Once the machinery is in place, the theorem is proved fairly easily.

This paper aims to present the main ideas involved in the proof of the transfer theorem. Since the method of proof is the same for the reals and the p-adics, many of the details have been omitted. These can be found for the reals in [19] and for the p-adics in [11]. The proof of the fundamental Lemma 3.1 is given in full, since it illustrates both the type of argument that is needed to give a satisfactory constructive proof and the changes that need to be made in passing from the reals to the p-adics. More details in the preliminary work on the p-adics have been included, as this material is not available in the literature.

2. The constructive p-adics

Before starting work on the transfer theorem, we need to establish some basic facts about the constructive p-adic numbers. In this section, the constructive p-adics are defined and they are shown to satisfy some of the algebraic properties of p-adically closed fields. As a result, the algebraic p-adics are a model of the classical theory of p-adically closed fields. We then focus on the algebraic p-adics, and show that various classical results can be proved constructively in this setting. These include cell decompositions and certain basic results for compact subsets of the algebraic p-adics. Theorem 2.11 is crucial to the latter, as it asserts the

existence of limits for bounded definable functions on the algebraic p-adics. It is also of independent interest. The proof is fairly technical, so it is postponed to the Appendix.

It will be assumed that the reader knows something of constructive real analysis as presented in [2]. The construction of the completion of an arbitrary metric space (X, ρ) given there could possibly be used for the p-adics. The elements of the completion are taken to be those Cauchy sequences from X which converge at the rate $\rho(x_m, x_n) \leq m^{-1} + n^{-1}$ for all positive integers m and n. However, the fact that the p-adic metric is topologically discrete makes it more natural to proceed with a different rate of convergence. Recall that the p-adic valuation, for a fixed prime p, is defined on the rationals by writing $0 \neq x \in \mathbb{Q}$ as $x = p^n r/s$, where $n, r, s \in \mathbb{Z}$ and $p \nmid rs$. The p-adic valuation is defined to be $|x|_p = p^{-n}$, and it is usual to write $n = \mathrm{ord}(x)$. That this function is a non-Archimedean valuation is easy to show, and additionally it satisfies the ultrametric inequality: for any $x, y \in \mathbb{Q}$, $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. The subscript p will normally be omitted, and $|\cdot|$ will be taken to denote the p-adic valuation unless otherwise indicated. The set of p-adic numbers is the completion of the rationals with respect to this valuation.

Definition 2.1. A *p-adic number* is a sequence of rationals $(x_n)_{n \geq 1}$ such that

$$|x_n - x_m| \leq p^{-\min\{n,m\}}, \quad \text{for all } n, m \in \mathbb{Z}^+.$$

Two p-adic numbers $x \equiv (x_n)$ and $y \equiv (y_n)$ are *equal*, $x = y$, if $|x_n - y_n| \leq p^{-n}$ for every $n \in \mathbb{Z}^+$, and are *apart*, $x \neq y$, if there is a positive integer A such that $|x_A - y_A| > p^{-A}$. The set of p-adic numbers is denoted by $\mathbb{Q}_p$, and the subset of p-adic numbers which are apart from zero is denoted by $\mathbb{Q}_p^*$.

The p-adic valuation on the rationals can be extended to the p-adics in a natural way. For $x \equiv (x_n)$, define

$$|x| = \lim_{n \to \infty} |x_n|,$$

where the limit is understood in the sense of the constructive reals. It is straightforward to show that this is a valuation on $\mathbb{Q}_p$ and satisfies the ultrametric inequality. In particular, if $x \neq 0$, then there is an integer A such that $|x| = |x_A| = |x_n|$ for every integer $n \geq A$. The valuation will be extended to $\mathbb{Q}_p^m$ by setting

$$|\boldsymbol{x}| = |(x_1, \ldots, x_m)| = \max\{|x_1|, \ldots, |x_m|\}.$$

The classical first-order theory of p-adically closed fields can be recursively axiomatised in a language containing the function symbols $+$, $-$, $\cdot$, constants 0, 1, binary predicates $\neq$ and V, and a family of unary predicates $\{P_n\}_{n \geq 2}$. The axioms (adapted from [18]) are those for a commutative ring of characteristic zero

and the universal closures of:

(i) $x \neq 0 \leftrightarrow \exists y\,(xy = 1)\ \&\ \neg(x \neq 0) \rightarrow x = 0$;

(ii) $V(x, y)\ \&\ V(y, z) \rightarrow V(x, z)$;

(iii) $V(x, y)\ \&\ V(x', y') \rightarrow V(xx', yy')$;

(iv) $V(x, y)\ \&\ V(x, y') \rightarrow V(x, y + y')$;

(v) $\neg V(p, 1)$;

(vi) $\neg V(1, x) \rightarrow V(px, 1)$;

(vii) $V(1, x) \rightarrow \bigvee_{i=0}^{p-1} V(p, x - i)$;

(viii)$_n$ $$\bigwedge_{i=0}^{n} V(1, x_i)\ \&\ V(1, y)\ \&\ V\Big(p, \sum_{i=0}^{n} x_i y^i\Big)\ \&\ V\Big(\sum_{i=1}^{n} i x_i y^{i-1}, 1\Big) \rightarrow \exists w \left[V(1, w)\ \&\ V(p, y - w)\ \&\ \sum_{i=0}^{n} x_i w^i = 0 \right];$$

(ix)$_{n\geqslant 2}$ $(y^n = x \rightarrow P_n(x))\ \&\ (P_n(x) \rightarrow \exists z\,(z^n = x))$;

(x)$_{n\geqslant 2}$ $$x \neq 0 \rightarrow \exists y \bigvee_{i=0}^{n=1} \bigvee_{\substack{a=1 \\ p \nmid a}}^{p^{2\mathrm{ord}(n)+1}} (P_n(y)\ \&\ ap^i y = x).$$

Axioms (ii)–(viii) express the fact that $|\cdot|$ is a p-valuation. (viii)$_n$ is Hensel's Lemma, (ix)$_n$ defines the P_n predicate, and (x)$_n$ says that the subgroup of nth powers has finite index in the multiplicative group $\mathbb{Q}_p^*$. Interpreted constructively, these axioms also hold in $\mathbb{Q}_p$, as is shown in the next proposition.

Proposition 2.2. *$(\mathbb{Q}_p, +, -, \cdot, 0, 1, \neq, V, \{P_n\}_{n\geqslant 2})$ is a model for the axioms* (i)–(x), *when $x \neq y$ is interpreted as 'x is apart from y', $V(x, y)$ is interpreted as $|x| \geqslant |y|$ and for each $n \geqslant 2$, $P_n(x)$ is interpreted as 'x is an nth power'.*

Proof. Addition, subtraction and multiplication are defined in obvious ways to make $\mathbb{Q}_p$ a commutative ring. It is then straightforward to define the inverse operation on $\mathbb{Q}_p^*$. The second conjunct of (i) is clear from the definition of apartness. (ii)–(iv) follow from the fact that $|\cdot|$ is a valuation with the ultrametric property. (v) holds by definition; $|p| = p^{-1}$ and $|1| = 1$. (vi) holds because, if $\neg(|x| \leqslant 1)$, then $|x| > 1$ as the p-adic topology is discrete. So $x \neq 0$, so $|x| = p^r$ for some $r \geqslant 1$, hence $|px| = p^{r-1} \geqslant 1$. (vii) follows from the fact that a p-adic which is apart from 0 can be written as an expansion in powers of p; if $x \in \mathbb{Q}_p^*$ with $|x| = p^{-r}$ and $k \geqslant r$, then there are $\tilde{x} \in \mathbb{Q}_p$ and integers $a_j \in \{0, 1, \ldots, p-1\}$ for $r \leqslant j \leqslant k$ such that $a_r \neq 0$, $|\tilde{x}| < p^{-k}$ and $x = \sum_{j=r}^{k} a_j p^j + \tilde{x}$. If $r > 0$, we can take $i = 0$ for (vii), and if $r = 0$, we can take $i = a_0$. If it is not known if $x \neq 0$ or not, then it must be the case that $|x| < |p|$, so $i = 0$ will do. (viii) is a corollary of Hensel's Lemma, proofs of which are usually given in a form which can easily be

made constructive. $(\text{ix})_n$ holds by definition of P_n. $(\text{x})_{n\geqslant 2}$ can be shown by writing $x = \sum_{j=r}^{2\text{ord}(n)+r} a_j p^j + \tilde{x}$, where $|x| = p^{-r}$, $|\tilde{x}| < p^{-(2\text{ord}(n)+r)}$ and $a_j \in \{0, 1, \ldots, p-1\}$. Let $a = \sum_{j=0}^{2\text{ord}(n)} a_{j+r} p^j$ and let i be the smallest positive integer such that n divides $r-i$. Then $0 \leqslant i \leqslant n-1$, $1 \leqslant a \leqslant p^{2\text{ord}(n)+1}$, $p \nmid a$ and the fact that $(ap^i)^{-1}x$ is an nth power can be shown using the following lemma. □

Lemma 2.3. *If $a \in \mathbb{Q}_p$ is an Nth power and $|b-a| < |N|^2 |a|$, then b is an Nth power.*

Proof. Apply Hensel's Lemma to the polynomial $f(X) = X^N - ba^{-1}$ (a is invertible as $a \neq 0$), with approximate solution 1. □

A first-order formula in the above language will be called a *p-adic algebraic formula.* A p-adic algebraic formula is a *simple formula* if it is a finite conjunction

$$\bigwedge_i \left[\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(\boldsymbol{x})) \to \bigvee_k \tilde{P}_{M_{ik}}(g_{ik}(\boldsymbol{x})) \right],$$

where the f_{ij} and g_{ik} are polynomials with integer coefficients, N_{ij} and M_{ik} are positive integers and $\tilde{P}_N$ is defined by

$$\tilde{P}_N(x) \leftrightarrow P_N(x) \,\&\, x \neq 0.$$

The transfer theorem applies to formulae constructed from simple formulae. Since classically the theory of p-adically closed fields admits elimination of quantifiers [13] and the predicate V can be eliminated in favour of the P_n predicates, every p-adic algebraic formula is, classically, equivalent to a simple formula. That this is not true constructively can be seen by considering the formula $(\tilde{P}_2(x^2) \to \bot) \to \bot$, which is not constructively equivalent to a simple formula. Corollary 3.5 uses the transfer theorem to show that the class of p-adic algebraic formulae which are constructively equivalent to simple formulae is quite large.

To consider a transfer theorem, we need to have a way of discussing the classical theory of p-adically closed fields from a constructive standpoint. This is provided by the algebraic p-adics; the elements of $\mathbb{Q}_p$ which satisfy a monic polynomial over $\mathbb{Q}$. In Propositions 2.5 and 2.6, it is shown that the algebraic p-adics Q_p form a discrete field (that is, $\forall x\, (x = 0 \vee x \neq 0)$ holds in Q_p) and hence conclude that the elementary theory of Q_p is the classical theory of p-adically closed fields.

Definition 2.4. $Q_p = \{x \in \mathbb{Q}_p : \exists n \geqslant 1\ \exists a_0, \ldots, a_{n-1} \in \mathbb{Q}\ (x^n + \sum_{i=0}^{n-1} a_i x^i = 0)\}$. The set of algebraic p-adics which are apart from 0 will be denoted by Q_p^*.

Proposition 2.5. $(Q_p, +, -, \cdot, 0, 1, \neq, V, \{P_n\}_{n\geqslant 2})$ *is a decidable substructure of* $(\mathbb{Q}_p, +, -, \cdot, 0, 1, \neq, V, \{P_n\}_{n\geqslant 2})$, *and satisfies the axioms* (i)–(x).

Proof. This can be proved in the same way as the corresponding result for the reals [19, Fact (A)]. The fact that the P_N predicates are decidable comes from the stronger version of (x):

$$(x)' \quad \exists y \bigvee_{i=0}^{n-1} \bigvee_{\substack{a=1 \\ p \nmid a}}^{p^{2\mathrm{ord}(N)+1}} (P_N(y) \,\&\, ap^i y = x),$$

which holds over Q_p. □

Proposition 2.6. *The elementary theory of Q_p is the classical theory of p-adically closed fields, and admits elimination of quantifiers.*

Proof. Once again, this is proved in the same way as the corresponding result for the reals [19, Fact (B)]. The fact that every prenex existential formula is equivalent to a quantifier-free formula is proved constructively in [10]. □

Proposition 2.7. *Q_p admits definable Skolem functions.*

Proof. This is proved constructively in [18]. □

The purpose of the next few paragraphs is to describe cylindrical algebraic decompositions (c.a.d.s), which are a useful tool for working with both the reals and the p-adics. First developed by Collins [8] to partition a real m-dimensional space into cells with special geometric properties, the geometry of these partitions can be used to give a constructive proof of quantifier elimination for the theory of real closed fields. Denef [10] used analogously defined cells to give a constructive proof of quantifier elimination for the theory of p-adically closed fields. Scowcroft and van den Dries [20] showed that one can construct a finite partition of a p-adic m-dimensional space into definable cells, and that this partition shares the nice geometric properties of Collins' c.a.d.s. The definition is by induction on m. A c.a.d. of Q_p^1 is a sequence of cells $\mathscr{C} = (C_{i,j})$, indexed by sequences of length two, and determined by a finite set of points $c_1, \ldots, c_k$. The cells $C_{i,0}$ consist of a single point:

$$C_{i,0} = \{c_i\}.$$

The cells $C_{i,j}$ with $j \neq 0$ are open sets:

$$C_{i,j} = \{x \in Q_p : |a_{ij1}| \,\square_{ij1}\, |x - c_i| \,\square_{ij2}\, |a_{ij2}| \,\&\, \tilde{P}_N(b_{ij}(x - c_i))\},$$

where $a_{ij1}, a_{ij2} \in Q_p$, and may not appear at all, $\square_{ij1}$ and $\square_{ij2}$ are $<$ or $\leqslant$ ($\square_{ij1}$ is $<$ if $a_{ij1} = 0$), N is fixed for the decomposition and b_{ij} is an element of a fixed set of representatives for the cosets of the Nth powers. For each cell C_{i0} the number of cells C_{ij} may vary. The cells are disjoint, and their union is Q_p. The index of a cell in Q_p^m will be a sequence of length $2m$ of nonnegative integers. Given a c.a.d. $\mathscr{C} = (C_\sigma)$ of Q_p^m, a c.a.d. of Q_p^{m+1} is obtained by partitioning each cylinder

$C_\sigma \times Q_p$ using finitely many definable, continuous functions $c_{\sigma,i}: C_\sigma \to Q_p$ which have the property that $c_{\sigma,i}(\boldsymbol{x}) \neq c_{\sigma,j}(\boldsymbol{x})$ for every $i \neq j$ and $\boldsymbol{x} \in C_\sigma$. The cells are defined as follows:

$$C_{\sigma^\frown(i,0)} = \{(\boldsymbol{x}, y) \in C_\sigma \times Q_p : y = c_{\sigma,i}(\boldsymbol{x})\},$$

$$C_{\sigma^\frown(i,j)} = \{(\boldsymbol{x}, y) \in C_\sigma \times Q_p : |a_{\sigma ij1}(\boldsymbol{x})| \,\square_{\sigma ij1}\, |y - c_{\sigma,i}(\boldsymbol{x})| \,\square_{\sigma ij2}\, |a_{\sigma ij2}(\boldsymbol{x})| \\ \& \tilde{P}_N(b_{\sigma ij}(y - c_{\sigma,i}(\boldsymbol{x})))\}, \quad \text{for } j \neq 0,$$

where $a_{\sigma ij1}$, $a_{\sigma ij2}: C_\sigma \to Q_p$ are continuous, definable functions which may or may not be present, $a_{\sigma ij1}$ is always or never zero on C_σ, $\square_{\sigma ij1}$ and $\square_{\sigma ij2}$ are $<$ or $\leqslant$ ($\square_{\sigma ij1}$ is $<$ if $a_{\sigma ij1} = 0$), and $b_{\sigma ij}$ is a coset representative. The cells partitioning any one cylinder $C_\sigma \times Q_p$ are disjoint and their union is $C_\sigma \times Q_p$. Hence all the cells of $\mathscr{C}$ are disjoint and their union is Q_p^{m+1}. The subscripts σ, i, j will be omitted wherever this is possible without ambiguity.

The rank of a cell C_σ of a c.a.d. of Q_p^m is the sequence of length m of zeros and ones defined by

$$(\mathrm{rk}(\sigma))_k = \begin{cases} 1, & \text{if } (\sigma)_{2k} \neq 0, \\ 0, & \text{if } (\sigma)_{2k} = 0, \end{cases}$$

for $1 \leqslant k \leqslant m$, where $(\sigma)_k$ is the kth element of the sequence σ. As members of ${}^m2$, the ranks may be ordered lexicographically. The dimension of a cell is defined to be

$$\dim(C_\sigma) = \dim(\sigma) = \sum_{k=1}^{m} (\mathrm{rk}(\sigma))_k.$$

A c.a.d. of Q_p^m induces a c.a.d. of Q_p^n for any $1 \leqslant n \leqslant m$; the induced c.a.d. can be found using the projection of Q_p^m onto Q_p^n which forgets the last $m - n$ coordinates. Two cells in Q_p^m project onto the same cell in Q_p^n if, and only if, their indices have the same initial segment of length $2n$; this initial segment is the index of the cell in the induced c.a.d. of Q_p^n. Another useful projection is $\pi_\sigma: C_\sigma \to Q_p^{\dim(\sigma)}$, the projection of C_σ onto those coordinate axes x_i for which $(\mathrm{rk}(\sigma))_i = 1$.

A c.a.d. of Q_p^m is said to be *invariant* with respect to an integer N and a polynomial $p(\boldsymbol{x}) \in Q_p[x_1, \ldots, x_m]$ (or with respect to a p-adic algebraic formula $M(\boldsymbol{x})$) if $p(\boldsymbol{x})$ takes values in a unique coset of the Nth powers and is always, or never, zero (or $M(\boldsymbol{x})$ has constant truth value) on each cell of the c.a.d.

Theorem 2.8. *For any $k \leqslant m$ there is a primitive-recursive algorithm which, from any integer N, and finite list of polynomials $p_i(\boldsymbol{x})$ and p-adic algebraic predicates $M_j(\boldsymbol{x})$ produces quantifier-free definitions of the cells of a c.a.d. of Q_p^k induced by a c.a.d. of Q_p^m invariant with respect to the p_i's, M_j's and N.*

Proof. This is a consequence of [20, Lemma 4.1], which is proved using Theorem 1.1 of the same paper and a result of Denef ([9], but proved constructively in

[10]). Only one point, in the proof of Theorem 1.1, needs constructive verification. The authors use the fact that an element of the algebraic closure of Q_p which is not in Q_p lies some positive distance away from Q_p. This fact can be established constructively for Q_p as follows. From [14, Theorem VI.3.5], there is a discrete algebraic closure Q_p^{alg} of the countable discrete field Q_p. Every element α of Q_p^{alg} satisfies a polynomial in $Q_p[X]$. By [14, Theorem VII.1.8] and Hensel's Lemma (which tell us that Q_p is factorial), this polynomial can be factored into irreducible components. So we can find a minimal polynomial $m_\alpha(X)$ for each α in Q_p^{alg}. Hence one can define a valuation on Q_p^{alg} in the usual way, by setting $|\alpha|^{\deg(m_\alpha)} = |\prod_{i=1}^{\deg(m_\alpha)} \alpha_i|$, where the α_i are the conjugates of $\alpha = \alpha_1$ over Q_p. For any $x \in Q_p$, the degree of the minimal polynomial for $\alpha - x$ is the same as the degree of the minimal polynomial for α, and x has only itself as conjugates. Hence

$$|\alpha - x|^{\deg(m_\alpha)} = \left| \prod_{i=1}^{\deg(m_\alpha)} (\alpha - x)_i \right| = \left| \prod_{i=1}^{\deg(m_\alpha)} (\alpha_i - x) \right| = |m_\alpha(x)|,$$

as this is precisely the definition of the conjugates α_i. Since $m_\alpha(X)$ is an irreducible polynomial, its discriminant D is apart from zero. Take m to be the least integer so that $p^m m_\alpha(X)$ has integral coefficients. Since $p^m m_\alpha(X)$ has no roots in Q_p, it follows from a corollary to Hensel's Lemma [6, p. 52] that $|p^m m_\alpha(x)| \geq |D|^2$ for every $x \in Q_p$ with $|x| \leq 1$, and hence for every $x \in Q_p$. Thus $|m_\alpha(x)| \geq p^m |D|^2$ for every $x \in Q_p$, so $|\alpha - x| \geq (p^m |D|^2)^{1/\deg(m_\alpha)}$ for every $x \in Q_p$. That is, the distance from α to every element of Q_p is bounded away from 0. □

The next two propositions describe further properties of the cells of a c.a.d. of Q_p^m. The first shows that the geometry of the cells is, in some sense, very simple, and describes how the cells fit together. The second shows that one may construct continuous functions with special properties relative to a c.a.d. These results correspond to [19, Facts (D) and (J)], respectively.

Proposition 2.9. (i) *$\pi_\sigma : C_\sigma \to Q_p^{\dim(\sigma)}$ is a continuous, continuously invertible mapping of C_σ onto $\pi_\sigma(C_\sigma)$, which is open in $Q_p^{\dim(\sigma)}$.*

(ii) *C_σ is closed in its union with the cells of higher rank, and this union is open in Q_p^m.*

Proof. The proof depends on properties of cells which are the same for both the reals and the p-adics, so does not need to be changed for the p-adic case. A proof of this result for the reals is given in [16, Lemma 2]. □

Proposition 2.10. *Let $\mathscr{C}$ be a c.a.d. of Q_p^{m+n}, C_σ a cell of the induced c.a.d. of Q_p^m, and $C_{\sigma^\frown\tau}$ a cell in $\mathscr{C}$. If $(\boldsymbol{x}, \boldsymbol{y}) \in C_{\sigma^\frown\tau}$, then there is a continuous, definable*

function $F_{\sigma^\frown\tau}$, defined on a neighborhood A of $\boldsymbol{x}$ in C_σ, such that $F_{\sigma^\frown\tau}(\boldsymbol{x}) = \boldsymbol{y}$ and the graph of $F_{\sigma^\frown\tau}$ is contained in $C_{\sigma^\frown\tau}$.

Proof. The proof of this result is very similar to the proof of the corresponding result for the reals [16, Lemma 3]. It is worth giving in full here because it illustrates the extra care which is necessitated by the addition of the $\tilde{P}_N$ predicates to the definitions of cells. The proof is by induction on n. The argument for the base case $n = 1$ is essentially the same as for the general case, so suppose that the result is true for c.a.d.s of Q_p^{m+n} with $m, n \geqslant 1$, and take $\mathscr{C}$ to be a c.a.d. of Q_p^{m+n+1}. Let $C_{\sigma^\frown\tau^\frown(i,j)}$ be a cell of $\mathscr{C}$ and $(\boldsymbol{x}, \boldsymbol{y}) \in C_{\sigma^\frown\tau^\frown(i,j)}$. For any $\boldsymbol{z} \in Q_p^{n+1}$, let $\boldsymbol{z}_1$ be the projection of $\boldsymbol{z}$ onto the first n coordinates and z_{n+1} the projection of $\boldsymbol{z}$ onto the last coordinate. By the induction hypothesis, there is a continuous, definable function $F_{\sigma^\frown\tau}$ from a neighborhood A_1 of $\boldsymbol{x}$ in C_σ such that $F_{\sigma^\frown\tau}(\boldsymbol{x}) = \boldsymbol{y}_1$ and the graph of $F_{\sigma^\frown\tau}$ is contained in $C_{\sigma^\frown\tau}$. If $j = 0$, then

$$C_{\sigma^\frown\tau^\frown(i,0)} = \{(\boldsymbol{w}, \boldsymbol{z}_1, z_{n+1}) \in C_{\sigma^\frown\tau} \times Q_p : z_{n+1} = c(\boldsymbol{w}, \boldsymbol{z}_1)\}.$$

$F_{\sigma^\frown\tau^\frown(i,0)}$ is defined on the neighborhood $A = A_1$ by

$$F_{\sigma^\frown\tau^\frown(i,0)}(\boldsymbol{w}) = (F_{\sigma^\frown\tau}(\boldsymbol{w}),\ c(\boldsymbol{w}, F_{\sigma^\frown}(\boldsymbol{w}))),$$

and the graph of $F_{\sigma^\frown\tau^\frown(i,0)}$ is clearly contained in $C_{\sigma^\frown\tau^\frown(i,0)}$. If $j \neq 0$, then

$$C_{\sigma^\frown\tau^\frown(i,j)} = \{(\boldsymbol{w}, \boldsymbol{z}_1, z_{n+1}) \in C_{\sigma^\frown\tau} \times Q_p : |a_1(\boldsymbol{w}, \boldsymbol{z}_1)| \,\square_1\, |z_{n+1} - c(\boldsymbol{w}, \boldsymbol{z}_1)| \,\square_2\, |a_2(\boldsymbol{w}, \boldsymbol{z}_1)| \ \&\ \tilde{P}_N(b(z_{n+1} - c(\boldsymbol{w}, \boldsymbol{z}_1)))\}.$$

Define

$$F_{\sigma^\frown\tau^\frown(i,j)}(\boldsymbol{w}) = (F_{\sigma^\frown\tau}(\boldsymbol{w}),\ y_{n+1}).$$

We have to find a neighborhood $A \subseteq A_1$ of $\boldsymbol{x}$ such that the graph of $F_{\sigma^\frown\tau^\frown(i,j)}$ is contained in $C_{\sigma^\frown\tau^\frown(i,j)}$. Since $(\boldsymbol{x}, \boldsymbol{y}) \in C_{\sigma^\frown\tau^\frown(i,j)}$, $b(y_{n+1} - c(\boldsymbol{x}, \boldsymbol{y}_1))$ is an Nth power. By Lemma 2.3, $b(y_{n+1} - c(\boldsymbol{w}, \boldsymbol{z}))$ is an Nth power for any $(\boldsymbol{w}, \boldsymbol{z}) \in C_{\sigma^\frown\tau}$ satisfying

$$|c(\boldsymbol{w}, \boldsymbol{z}) - c(\boldsymbol{x}, \boldsymbol{y}_1)| < |b|^{-1} |N|^2 |y_{n+1} - c(\boldsymbol{x}, \boldsymbol{y}_1)|.$$

In this case, $|y_{n+1} - c(\boldsymbol{x}, \boldsymbol{y}_1)| = |y_{n+1} - c(\boldsymbol{w}, \boldsymbol{z})|$, so $|a_1(\boldsymbol{w}, \boldsymbol{z})| \,\square_1\, |y_{n+1} - c(\boldsymbol{w}, \boldsymbol{z})| \,\square_2\, |a_2(\boldsymbol{w}, \boldsymbol{z})|$, provided $|a_i(\boldsymbol{w}, \boldsymbol{z})| = |a_i(\boldsymbol{x}, \boldsymbol{y}_1)|$ for $i = 1, 2$. This is assured if a_i is identically zero or

$$|a_i(\boldsymbol{w}, \boldsymbol{z}) - a_i(x, \boldsymbol{y}_1)| < |a_i(\boldsymbol{x}, \boldsymbol{y}_1)|,$$

which is possible as the a_i are always or never zero on $C_{\sigma^\frown\tau}$. Since the functions c, a_1, a_2 are continuous, there is a $\delta \in Q_p^*$ such that, if $|(\boldsymbol{w}, \boldsymbol{z}) - (\boldsymbol{x}, \boldsymbol{y}_1)| < |\delta|$, then all of the displayed conditions above hold. $F_{\sigma^\frown\tau}$ is continuous on A_1, so there is an open set $A \subseteq A_1$ such that $|(\boldsymbol{w}, F_{\sigma^\frown\tau}(\boldsymbol{w})) - (\boldsymbol{x}, \boldsymbol{y})| < |\delta|$ for every $\boldsymbol{w} \in A$. The above discussion then shows that $(\boldsymbol{w}, F_{\sigma^\frown\tau^\frown(i,j)}(\boldsymbol{w})) \in C_{\sigma^\frown\tau^\frown(i,j)}$ for every $\boldsymbol{w} \in A$. $\square$

The next theorem corresponds to the result for the reals [19, Fact (G)] that a bounded, definable function from the interval $(0, 1]$ in the algebraic reals has a well-defined limit at 0. One can replace the 'interval $(0, 1]$' by any bounded definable subset A with the property that A has interior, has 0 as a limit point and is a subset of the set of squares in R. The analogy with the p-adic result then becomes clear; the proof of Theorem 2.11 shows that a bounded definable function on an open ball in Q_p around 0 has a well-defined limit at 0 on an open subset of the set of Nth powers, for some N. Scowcroft gives a concise proof of his result which does not, however, carry over to the p-adics, since it uses the ordering on the reals in an essential way. The proof given here would also work for the reals, but since the proof itself is not essential to what follows, it is postponed to the Appendix.

Theorem 2.11. *Let $f: U \to Q_p$ be a bounded, definable function whose domain includes a punctured open ball $U \subset Q_p$ around the origin. One can find an open set $A \subseteq U$ with $0 \in \mathrm{cl}(A)$ such that $\lim_{x \to 0, x \in A} f(x)$ exists in Q_p.*

The next two propositions correspond exactly to results for the reals [19, Facts (H) and (I)]. Given Theorem 2.11, the proofs are essentially unchanged. They show that certain classical results on compact sets hold constructively in the algebraic p-adics for definable sets.

Definition 2.12. (i) A set $C \subset Q_p^m$ is taken to be *compact* if it is definable, bounded and closed in Q_p^m.

(ii) A p-adic algebraic formula $\varphi(x, y, \delta)$ is said to be *monotone* in δ if

$$\forall x, y, \delta, \theta\, ((0 < |\theta| \leqslant |\delta| \,\&\, \varphi(x, y, \delta)) \to \varphi(x, y, \theta))$$

holds over Q_p.

Proposition 2.13. *If $C \subset Q_p^m$ is compact and $f: C \to Q_p^n$ is a definable, continuous function, then $f(C)$ is compact.*

Proposition 2.14. *If $C \subset Q_p^m$ is compact, $\varphi(x, z, \delta)$ is monotone in δ and*

$$\forall x \in C\, \exists \delta \in Q_p^*\, \forall y \in Q_p\, (|y - x| < |\delta| \to \varphi(y, z, \delta))$$

holds over Q_p, then there is a $\delta \in Q_p^*$ such that

$$\forall x \in C\, \varphi(x, z, \delta)$$

holds over Q_p.

The final result of this section, the so-called 'finiteness theorem' of semi-algebraic geometry, says that an open definable set can be written in a form which makes it obvious that it is open. A constructive proof of this result can be found in [4].

Proposition 2.15. *For any open definable set $S \subseteq Q_p^m$ there is an integer N such that S can be written as a finite union of finite intersections of sets of the form $\{x \in Q_p^m : \tilde{P}_N(f(x))\}$, where $f(x)$ is a polynomial over Q_p.*

3. The main constructive theorem

This section shows how one may prove that certain p-adic algebraic formulae made up of simple formulae are constructively valid.

The following fundamental lemma constructs a link between points $\boldsymbol{x} \in \mathbb{Q}_p^m$ obeying a simple formula M, and sequences of points in Q_p^m which obey M and converge to $\boldsymbol{x}$.

Lemma 3.1. *Given a c.a.d. $\mathscr{C}$ of Q_p^m and an $\boldsymbol{x} \in \mathbb{Q}_p^m$ one may generate a sequence $(\boldsymbol{y}_k)_{k \geq 1}$ in Q_p^m which converges to $\boldsymbol{x}$ and has the following properties.*

(i) $|\boldsymbol{y}_k - \boldsymbol{y}_l| \leq p^{-\min\{k,l\}}$ *for every* $k, l \geq 1$.

(ii) *If $\boldsymbol{y}_k$ and $\boldsymbol{y}_{k+1}$ belong to different cells in $\mathscr{C}$, then $\boldsymbol{y}_{k+1}$'s cell has higher rank than $\boldsymbol{y}_k$'s cell.*

(iii) *If $\boldsymbol{y}_k$ belongs to a cell C_σ, then there is a compact set $C \subseteq C_\sigma$ such that, for any $l \geq k$, if $\boldsymbol{y}_l \in C_\sigma$, then $\boldsymbol{y}_l \in C$.*

(iv) *Let $M(z_1, \ldots, z_m)$ be the predicate*

$$\bigwedge_i \left[\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(\boldsymbol{z})) \rightarrow \bigvee_k \tilde{P}_{M_{ik}}(g_{ik}(\boldsymbol{z})) \right]$$

($f_{ij}, g_{ik} \in \mathbb{Q}[Z]$) and suppose that $\mathscr{C}$ is invariant with respect to the polynomials f_{ij} and g_{ik}, and the integers N_{ij} and M_{ik}.

(a) *If $M(\boldsymbol{x})$, then one may generate a subsequence $(\boldsymbol{y}_{n_k})_{k \geq 1}$ of $(\boldsymbol{y}_k)_{k \geq 1}$ such that $M(\boldsymbol{y}_{n_k})$ holds for every $k \geq 1$.*

(b) *If $M(\boldsymbol{y}_k)$ for every $k \geq 1$, then $M(\boldsymbol{x})$.*

Proof. The proof of (i)–(iii) is by induction on m. We start with the sequence $(\boldsymbol{x}_k)$ of rational points with which $\boldsymbol{x}$ is initially presented. This sequence satisfies (i) but cannot be expected to satisfy (ii), so we choose the sequence $(\boldsymbol{y}_k)$ to be algebraic points which lie close enough to the sequence $(\boldsymbol{x}_k)$ that the two sequences have the same limit. To satisfy (ii), each $\boldsymbol{y}_k$ should be in a cell of minimal rank amongst those cells intersecting a ball of radius p^{-k} around $\boldsymbol{x}_k$. This ensures that the rank of cells cannot decrease from $\boldsymbol{y}_k$ to $\boldsymbol{y}_{k+1}$. To make sure that $\boldsymbol{y}_{k+1}$ is not in a different cell of the same rank to that containing $\boldsymbol{y}_k$, the cell of minimal rank should be unique. This is ensured by introducing a delay factor: $\boldsymbol{y}_k$ is chosen to lie close to $\boldsymbol{x}_{k+n}$ for some appropriate n. This method of choosing the cell in which $\boldsymbol{y}_k$ lies also ensures that $\boldsymbol{y}_{k+1}$ is only in a different cell to the cell C_σ containing $\boldsymbol{y}_k$ if the sequence $(\boldsymbol{x}_k)$ is bounded away from C_σ. This makes it possible to satisfy (iii). The basic outline of the proof is the same as that of the

corresponding result for the reals. The details, however, differ enough to make it worthwhile reproducing the argument in full. This will also make it possible to omit details of some of the later proofs.

The case $m = 1$ illustrates the process described above very clearly. The set of single point cells of $\mathscr{C}$ is the discrete set of points $\{c_1, \ldots, c_r\}$ with $|c_i - c_j| > p^{-\alpha}$, say, for every pair $i \neq j$. The sequence $(y_k)_{k \geq 1}$ is defined inductively. If there is an i such that $|x_{\alpha+1} - c_i| \leq p^{-(\alpha+1)}$, then let $y_1 = c_i$. (It is easy to see that c_i is unique, so y_1 is well-defined.) As long as $|x_{\alpha+k} - c_i| \leq p^{-(\alpha+k)}$, let y_k be c_i. If $y_k = c_i$ and $y_{k+1} = c_j$, it follows from the ultrametric property and the definition of α that $c_i = c_j$. Thus, this part of the sequence satisfies (ii). If there is an integer l for which $|x_{\alpha+l} - c_i| > p^{-(\alpha+l)}$ for every i, one can define

$$l_0 = \mu l \geq 1\left[\bigwedge_{j=1}^{n} |x_{\alpha+l} - c_j| > p^{-(\alpha+l)}\right],$$

and $k_0 = l_0 + 2n$, where $n = \operatorname{ord}(N)$ and N is the integer (a least common multiple of the N_{ij}'s and M_{ik}'s) which appears as the $\tilde{P}_N$ predicate in the definition of the cells of $\mathscr{C}$. Let

$$y_k = x_{\alpha+2n+k}, \quad \text{for every } k \geq l_0.$$

The claim is that the sequence $(y_l)_{l \geq l_0} = (x_{\alpha+k})_{k \geq k_0}$ lies in one cell of $\mathscr{C}$. Suppose

$$C_\sigma = \{z \in Q_p : |a_1| \square_1 |z - c_j| \square_2 |a_2| \ \& \ \tilde{P}_N(b(z - c_j))\}$$

is the cell containing $x_{\alpha+k_0}$. Since for every $k \geq k_0$,

$$|x_{\alpha+k} - x_{\alpha+k_0}| \leq p^{-(\alpha+k_0)} = p^{-2n} p^{-(\alpha+l_0)} < |N|^2 |x_{\alpha+k_0} - c_j|$$

(by definition of l_0), and $b(x_{\alpha+k_0} - c_j)$ is a nonzero Nth power, it follows from Lemma 2.3 that $b(x_{\alpha+k} - c_j)$ is a nonzero Nth power. It also follows that $|x_{\alpha+k} - c_j| = |x_{\alpha+k_0} - c_j|$ and hence $|a_1| \square_1 |x_{\alpha+k} - c_j| \square_2 |a_2|$ for $k \geq k_0$. Thus $x_{\alpha+k} \in C_\sigma$ for every $k \geq k_0$ and the claim is shown. Hence the sequence $(y_k)_{k \geq 1}$ satisfies (ii). The fact that the sequence satisfies (i) is immediate from the construction. To show that (iii) holds for this sequence, one may let $C = \{c_i\}$ as long as $y_k = c_i$. For $k \geq l_0$,

$$y_k \in C = \{z \in Q_p^n : |z - c_j| = |x_{\alpha+k_0} - c_j| \ \& \ \tilde{P}_N(b(z - c_j))\},$$

which is a compact subset of C_σ.

Assume now that $m \geq 1$ and that (i)–(iii) hold for c.a.d.s of Q_p^k when $k \leq m$. To extend the result to c.a.d.s of Q_p^{m+1}, the idea is to apply the above argument to the last coordinate of $\boldsymbol{x}$. Let $\Pi_0 : \mathbb{Q}_p^{m+1} \to \mathbb{Q}_p^m$ be projection onto the first m coordinate axes, and $\Pi_1 : \mathbb{Q}_p^{m+1} \to \mathbb{Q}_p$ be projection onto the last coordinate axis. Let $\boldsymbol{x} = (\boldsymbol{x}_k)$ and apply the induction hypothesis to get a sequence $(\boldsymbol{y}_k)$ which converges to $\Pi_0(\boldsymbol{x})$ and obeys (i)–(iii) relative to the c.a.d. of Q_p^m induced by $\mathscr{C}$. Letting $z_k = \Pi_1(\boldsymbol{x}_k)$, for $k \geq 1$, it is easy to show that the sequence $((\boldsymbol{y}_k, z_k))_{k \geq 1}$ converges to $\boldsymbol{x}$ at the required rate. The process of finding a new sequence $(\boldsymbol{w}_k)$

which will obey (i)–(iii) is started using information about the cell containing y_1. If the sequence (y_k) changes cell, the process is iterated with information about the new cell. (ii) ensures that this happens only finitely many times.

Let C_σ be the cell containing y_1, and let C be the compact subset which contains all of the y_k's which lie in C_σ. Since the continuous functions $c_i: C_\sigma \to Q_p$ are apart, by Proposition 2.14 there is a positive integer α such that, for every $u \in C$ and $j \neq i$, $|c_i(u) - c_j(u)| > p^{-\alpha}$. Similarly, the continuous functions c_i are uniformly continuous on C, so there is a positive integer δ such that, for every i and every $u, v \in C$, if $|u - v| < p^{-\delta}$, then $|c_i(u) - c_i(v)| < p^{-\alpha}$. Furthermore, by taking a subsequence if necessary, one can assume that $|c_i(y_k) - c_i(y_l)| \leq p^{-\min(k,l)}$ for any $y_k, y_l \in C_\sigma$.

To start computing the w_k's, let $k_0 = \max\{\alpha, \delta\}$. If $y_{k_0+1} \notin C_\sigma$, then start again with the cell C_τ containing y_{k_0+1}; find the new α, δ, k_0 and proceed as below. As long as $y_{k_0+k} \in C_\sigma$, w_k is computed by setting

$$w_k = (y_{k_0+k}, c_i(y_{k_0+k})), \quad \text{where } |z_{k_0+k} - c_i(y_{k_0+k})| \leq p^{-(k_0+k)},$$

if there is such an i. If there is no such i, then w_k is given in the next paragraph. As for the $m = 1$ case, it follows from the ultrametric property and the definition of k_0 that w_k is well-defined and, as long as w_k is defined in this way, the sequence does not change cell. The w_k are contained in the graph of c_i on C which is a compact set by Proposition 2.13, as C is compact.

Now suppose there is a least $k_1 \geq 1$ such that $y_{k_0+k_1} \in C_\sigma$ and $|z_{k_0+k_1} - c_i(y_{k_0+k_1})| > p^{-(k_0+k_1)}$, for every i. Then define

$$w_k = (y_{k_0+2n+k}, z_{k_0+2n+k})$$

for every $k \geq k_1$ such that $y_{k_0+2n+k} \in C_\sigma$ (where still $n = \operatorname{ord}(N)$). The claim is that the sequence $(w_k)_{k \geq k_1}$ stays in the same cell as long as the sequence $(y_{k_0+2n+k})_{k \geq k_0}$ stays in the same cell. Suppose $(y_{k_0+2n+k_1}, z_{k_0+2n+k_1}) \in C_{\sigma^\frown(i,j)}$ where

$$C_{\sigma^\frown(i,j)} = \{(y, z) \in C_\sigma \times Q_p : |a_1(y)| \,\square_1\, |z - c_i(y)| \,\square_2\, |a_2(y)| \\ \& \tilde{P}_N(b(z - c_i(y)))\}.$$

Since $b(z^{k_0+2n+k_1} - c_i(y_{k_0+2n+k_1}))$ is a nonzero Nth power and

$$\begin{aligned} &|b(z_{k_0+2n+k_1} - c_i(y_{k_0+2n+k_1})) - b(z_{k_0+2n+k} - c_i(y_{k_0+2n+k}))| \\ &\quad \leq |b|\, p^{-(k_0+2n+k_1)} \\ &\quad < |b|\, p^{-2n}\, |z_{k_0+2n+k_1} - c_i(y_{k_0+2n+k_1})| \end{aligned}$$

(by the ultrametric property and the assumptions on the rate of convergence of the sequence $(c_i(y_k))$ in C_σ), it follows from Lemma 2.3 that $b(z_{k_0+2n+k} - c_i(y_{k_0+2n+k}))$ is an nth power. It also follows that

$$|z_{k_0+2n+k} - c_i(y_{k_0+2n+k})| = |z_{k_0+2n+k_1} - c_i(y_{k_0+2n+k_1})|.$$

Since the functions a_1 and a_2 are continuous (and a_1 is always or never zero on C_σ), they are uniformly continuous on C, so there is a $\delta \in Q_p^*$ such that, if

$|y - y'| < |\delta|$ for any $y, y' \in C$, then $|a_1(y)| = |a_1(y')|$ and $|a_2(y)| = |a_2(y')|$. Let $k_2 \geqslant 2n$ be such that $p^{-(k_0+k_1+k_2)} \leqslant |\delta|$. Adjust the definition of w_k to include k_2:

$$w_k = (y_{k_0+k_2+k}, z_{k_0+k_2+k})$$

for $k \geqslant k_1$ such that $y_{k_0+k_2+k} \in C_\sigma$. Then

$$|a_1(y_{k_0+k_2+k})| \square_1 |z_{k_0+k_2+k} - c_i(y_{k_0+k_2+k})| \square_2 |a_2(y_{k_0+k_2+k})|,$$

and hence $w_k \in C_\sigma$. The above argument shows further that w_k is in the compact set $C' \subseteq C_\sigma$ defined by

$$C' = \{(y, z) \in C \times Q_p : |z - c_i(y)| = |z_{k_0+k_1+k_2} - c_i(y_{k_0+k_1+k_2})| \\ \& \tilde{P}_N(b(z - c_i(y)))\}.$$

This part of the sequence thus satisfies (ii) and (iii).

Once $y_{k_0+k_2+k} \notin C_\sigma$, the construction of the sequence (w_k) continues as at the beginning of this argument. Provided (y_k) remains in the same cell, the construction so far shows that the sequence (w_k) only changes cell to a cell of higher rank. If (y_k) changes cell, then by the induction hypothesis it changes to a cell of higher rank, and hence the sequence (w_k) changes to a cell of higher rank (recall that the ranks are ordered lexicographically). Thus (ii) holds. That (iii) holds is given in the construction, so it only remains to check (i). This follows easily from the rate of convergence of the sequence $((y_k, z_k))$, the uniform continuity of the functions c_i and the fact that a point $c_i(y_k)$ is only used if it is sufficiently close to z_k. This finishes the proof of (i)–(iii).

To prove (iv)(a), we construct a subsequence $(y_{k_r})_{r \geqslant 1}$ of $(y_k)_{k \geqslant 1}$, every term of which obeys M. Suppose y_{k_r} obeys M for all $r < s$ and the problem is to find k_s so that $M(y_{k_s})$. Let $u = y_{k_{r-1}+1}$ (or y_1 if $s = 1$). If $M(u)$, then $k_s = k_{r-1} + 1$ (or 1 if $s = 1$). If $\neg M(u)$, then, since $u \in Q_p^m$ and $Th(Q_p)$ is decidable, there is an i for which

$$\neg\left[\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(u)) \to \bigvee_l \tilde{P}_{M_{il}}(g_{il}(u))\right]$$

holds in Q_p, and hence

$$\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(u)) \;\&\; \bigwedge_l \neg\tilde{P}_{M_{il}}(g_{il}(u)).$$

If C_σ is u's cell in $\mathscr{C}$, (iii) provides a compact $C \subseteq C_\sigma$ containing u and all subsequent y_k's which are in C_σ. Because $\mathscr{C}$ is invariant with respect to the f's, g's, N's and M's,

$$\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(y_k)) \;\&\; \bigwedge_l \neg\tilde{P}_{M_{il}}(g_{il}(y_k))$$

for every $y_k \in C_\sigma$. Thus, it seems as though it might not be possible to find another y_k for which $M(y_k)$, as the sequence might not change cell again. However, one can show that the sequence must change cell, by considering

$y_\sigma = \lim_{k\to\infty, y_k\in C_\sigma} y_k$. Notice that $y_\sigma = y_a$ if there is an integer a such that $y_{a+1} \in C'_\sigma$ and $\mathrm{rk}(\sigma') > \mathrm{rk}(\sigma)$. The next paragraphs show that there is such an a.

For every $y_k \in C$, $f_{ij}(y_k) \neq 0$ for every j. Since C is compact, there is an integer α such that $|f_{ij}(y_k)| > p^{-\alpha}$ for every j and every $y_k \in C$. Taking limits, $|f_{ij}(y_\sigma)| > p^{-\alpha}$. Thus, since $f_{ij}(y_\sigma) \neq 0$, taking limits again gives that $\tilde{P}_{N_{ij}}(f_{ij}(y_\sigma))$, for every j. Since $\bigwedge_l \neg\tilde{P}_{M_{il}}(g_{il}(y_k))$ is a closed condition, this also holds in the limit. So

$$\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(y_\sigma)) \,\&\, \bigwedge_l \neg\tilde{P}_{M_{il}}(g_{il}(y))$$

holds, and hence $\neg M(y_\sigma)$. Since $M(x)$ holds, clearly $\neg(x = y_\sigma)$. This is not quite enough, however, because one needs to know k for which y_k jumps to a new cell.

Since f_{ij} is continuous, by Lemma 2.3 one can find an integer β such that, if $|z - y_\sigma| \leq p^{-\beta}$, then $\bigwedge_j \tilde{P}_N(f_{ij}(z))$. If $|x - y_\sigma| > p^{-\beta}$, then also $|y_\sigma - y_\beta| > p^{-\beta}$, as $|x - y_\beta| \leq p^{-\beta}$, so y_β must be in a different cell, by definition of y_σ. Then one can take $k_s = \beta$, if $M(y_\beta)$ and otherwise repeat the arguments. If $\neg(|x - y_\sigma| > p^{-\beta})$, then, since the p-adic topology is discrete, $|x - y_\sigma| \leq p^{-\beta}$, so $\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(x))$ holds. Since $M(x)$ holds, there is an l such that $\tilde{P}_{M_{il}}(g_{il}(x))$ holds. $|g_{il}(x)| = p^{-a}$ for some integer a. Since g_{il} is continuous, one can find an integer γ such that, if $|z - x| \leq p^{-\gamma}$, then $|g_{il}(z) - g_{il}(x)| < p^{-a}|M_{il}|^2 \leq p^{-a}$. If $|x - y_\sigma| \leq p^{-\gamma}$, then $|g_{il}(y_\sigma)| = |g_{il}(x)| = p^{-a}$ and, by Lemma 2.3, $g_{il}(y_\sigma)$ is an M_{il}th power. But since $\neg\tilde{P}_{M_{il}}(g_{il}(y_\sigma))$ holds, it must be the case that $|x - y_\sigma| > p^{-\gamma}$. So, as before, y_γ is in a different cell, and one can put $k_s = \gamma$ if $M(y_\gamma)$. If not, then the argument can be repeated. Since the sequence can only change cell at most $2^m - 1$ times, eventually one will find k_s.

(iv)(b) is proved by a similar argument. If $\bigwedge_j \tilde{P}_{N_{ij}}(f_{ij}(x))$, then there is an integer α such that, if $|z - x| \leq p^{-\alpha}$, then $\bigwedge \tilde{P}_{N_{ij}}(f_{ij}(z))$. For $k \geq \alpha + 1$, y_k lies in this region. Let C_σ be the cell containing $y_{\alpha+1}$, and C the compact set given by (iii). Since $M(y_{\alpha+1})$ holds, there is an l such that $\tilde{P}_{M_{il}}(g_{il}(y_{\alpha+1}))$, and since $\mathscr{C}$ is invariant with respect to the f's and g's, this holds throughout C. Let $y_o = \lim_{k\to\infty, y_k\in C_\sigma} y_k$. As C is compact, the function $g_{il}(y_k)$ is bounded away from zero on C, so the property of being a nonzero M_{il}th power carries over to the limit, i.e., $\tilde{P}_{M_{il}}(g_{il}(y_\alpha))$. There is an integer β such that if $|z - y_\sigma| \leq p^{-\beta}$, then $\tilde{P}_{M_{il}}(g_{il}(z))$. Thus, if $|x - y_\sigma| \leq p^{-\beta}$, then $\tilde{P}_{M_{il}}(g_{il}(x))$, and so $M(x)$ holds, as required. If $|x - y_\sigma| > p^{-\beta}$, then $x \neq y_\sigma$ and so y_β must be in a new cell. As the sequence can only change cell at most $2^m - 1$ times, eventually one gets $M(x)$ to hold. □

It is useful to note, for later reference, that (iv) does not depend on the specific rate of convergence in (i). Once the sequence (y_k) is known to converge, (iv) follows from (ii) and (iii).

The next lemma describes an algorithm which, from simple formulae $M(x)$ and $N(x, y)$, produces a p-adic algebraic predicate $G(x, y)$. G has a continuity property which N may lack, and it is this continuity which will characterize what is required for the sentence $\forall x\,(M(x) \to \exists y\, N(x, y))$ to hold over $\mathbb{Q}_p$.

Lemma 3.2. *Let $M(x_1, \ldots, x_m)$ and $N(x_1, \ldots, x_m, y_1, \ldots, y_n)$ be p-adic algebraic formulae and $\mathscr{C}$ be a c.a.d. of Q_p^{m+n} invariant with respect to M and N. From M and N one can generate a formula $G(\boldsymbol{x}, \boldsymbol{y})$ and a c.a.d. $\mathscr{C}^*$ which have the following properties. $\mathscr{C}^*$ refines $\mathscr{C}$ and if $(\boldsymbol{x}_0, \boldsymbol{y}_0) \in Q_p^{m+n}$ and $\boldsymbol{x}_0$ belongs to a cell C_σ of the c.a.d. of Q_p^m induced by $\mathscr{C}^*$, then $Th(Q_p)$ implies that*

$$G(\boldsymbol{x}_0, \boldsymbol{y}_0) \leftrightarrow M(\boldsymbol{x}_0) \,\&\, N(\boldsymbol{x}_0, \boldsymbol{y}_0) \,\&\, \forall \varepsilon \neq 0\, \exists \delta \neq 0\, \forall \boldsymbol{u} \\ [|\boldsymbol{u} - \boldsymbol{x}_0| < |\delta| \,\&\, M(\boldsymbol{u}) \,\&\, \neg D_\sigma(\boldsymbol{u}) \rightarrow \exists \boldsymbol{v}\, (|\boldsymbol{v} - \boldsymbol{y}_0| < |\varepsilon| \,\&\, G(\boldsymbol{u}, \boldsymbol{v}))], \tag{1}$$

where $D_\sigma(\boldsymbol{x})$ is a p-adic algebraic definition of C_σ. Any c.a.d. of Q_p^{m+n} which refines $\mathscr{C}^*$ also obeys (1).

Proof. The proof of this lemma depends only on properties of c.a.d.s which are the same for both the reals and the p-adics, so I shall only give an outline here. The detailed construction of G is originally given in [17, p. 282], and the proof that it satisfies (1) is given in [19, Appendix 1]. These arguments are amalgamated in [11]. The proof is by induction on m, the number of free $\boldsymbol{x}$-variables in the formulae M and N. At each inductive step, one uses a downward induction on θ, the ranks of cells in the c.a.d. $\mathscr{C}'$ of Q_p^m induced by $\mathscr{C}$, to define increasingly refined sequences $(\mathscr{C}^\theta)$ of c.a.d.s of Q_p^{m+n} and (G_θ) of p-adic algebraic formulae. G_θ is chosen to satisfy (1) with respect to $\mathscr{C}^\theta$ for points $\boldsymbol{x}_0$ in cells (of $\mathscr{C}$) of rank greater than or equal to θ. The required $\mathscr{C}^*$ and G are thus given by $\mathscr{C}^0$ and G_0.

If $\boldsymbol{x}_0$ is in a cell C of rank $\theta < \mathbf{1}$, then $\dim(C) = d < m$. The trick is to quantify out the $m - d$ coordinates of $\boldsymbol{x}_0$ which are given by continuous functions of the other coordinates, and consider two new formulae $\hat{M}(\hat{\boldsymbol{x}})$ and $\hat{N}(\hat{\boldsymbol{x}}, \boldsymbol{y})$ with only d free $\boldsymbol{x}$-variables. The new formula $\hat{M}(\hat{\boldsymbol{x}})$ is defined to hold if $\boldsymbol{x}$ is in a cell of rank θ and $M(\boldsymbol{x})$ holds. The new formula $\hat{N}(\hat{\boldsymbol{x}}, \boldsymbol{y})$ states the condition (1) which $G(\boldsymbol{x}, \boldsymbol{y})$ should satisfy for points $(\boldsymbol{x}, \boldsymbol{y})$ with $\boldsymbol{x}$ in a cell of rank θ. Since the $\hat{M}$ and $\hat{N}$ have only d free $\boldsymbol{x}$-variables, the induction hypothesis on m gives a c.a.d. $\hat{\mathscr{C}}$ of Q_p^{d+n} and a formula $\hat{G}$ which satisfy the statement of the lemma. $\mathscr{C}^\theta$ is now taken to be a c.a.d. which is a refinement of $\mathscr{C}^{\mathrm{succ}(\theta)}$ (where $\mathrm{succ}(\theta)$ is the successor of θ in the lexicographic ordering of ${}^m2$) and is invariant with respect to the formulae defining the cells of $\hat{\mathscr{C}}$. G_θ combines in an obvious way the formulae $\hat{G}$ for each cell of rank θ and it is straightforward, though lengthy, to check that $\mathscr{C}^\theta$ and G_θ are as required. □

The proof of Theorem 3.4 actually uses the following property of G, known as G's continuity property. The proof is immediate from Lemma 3.2 and Proposition 2.10.

Corollary 3.3. *In the same situation as the previous lemma,*

$$G(\boldsymbol{x}_0, \boldsymbol{y}_0) \leftrightarrow M(\boldsymbol{x}_0) \,\&\, N(\boldsymbol{x}_0, \boldsymbol{y}_0) \,\&\, \forall \varepsilon \neq 0\, \exists \delta \neq 0\, \forall \boldsymbol{u} \\ [|\boldsymbol{u} - \boldsymbol{x}_0| < |\delta| \,\&\, M(\boldsymbol{u}) \rightarrow \exists \boldsymbol{v} (|\boldsymbol{v} - \boldsymbol{y}_0| < |\varepsilon| \,\&\, G(\boldsymbol{u}, \boldsymbol{v}))].$$

The machinery is now in place to prove the main constructive result. Let $M(\boldsymbol{x})$ and $N(\boldsymbol{x}, \boldsymbol{y})$ be simple formulae and $G(\boldsymbol{x}, \boldsymbol{y})$ the formula generated in Lemma 3.2, where $\boldsymbol{x} = (x_1, \ldots, x_m)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$.

Theorem 3.4. *If*

$$\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y})) \tag{2}$$

holds over Q_p, *then*

$$\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y})) \tag{3}$$

holds over $\mathbb{Q}_p$.

Proof. Once again, the proof is very similar to the proof of the corresponding result for the reals. The details differ somewhat because of the differences between the real and p-adic valuations, but these changes are easy to make by comparing the real and p-adic proofs of Lemma 3.1. In outline, the proof is as follows.

Let $\mathscr{C}$ be a c.a.d. of Q_p^{m+n}, invariant with respect to G and the terms and rth power conditions in M and N. Consider $\boldsymbol{x} \in \mathbb{Q}_p^m$ such that $M(\boldsymbol{x})$ holds. By Lemma 3.1, there is a sequence $(\boldsymbol{x}_k)$ from Q_p^m converging to $\boldsymbol{x}$ such that $M(\boldsymbol{x}_k)$ holds for each k. By hypothesis, there is a sequence $(\boldsymbol{y}_k)$ (not necessarily convergent) from Q_p^n such that $G(\boldsymbol{x}_k, \boldsymbol{y}_k)$ holds and so, in particular, $N(\boldsymbol{x}_k, \boldsymbol{y}_k)$ holds. Suppose for a moment that all of the $\boldsymbol{x}_k$ lie in one cell C_σ of the c.a.d. $\mathscr{C}'$ of Q_p^m induced by $\mathscr{C}$. Then by Proposition 2.10 there is a continuous function F whose graph is contained in a cell $C_{\sigma\hat{}\tau}$ of $\mathscr{C}$ on which N holds. Since the x_k's in C_σ are contained in a compact subset C of C_σ, F is uniformly continuous on C (Proposition 2.14) and the graph of F is a compact subset of $C_{\sigma\hat{}\tau}$ (Proposition 2.13). So one can choose a subsequence $(\boldsymbol{x}_{n_k})$ of $(\boldsymbol{x}_k)$ so that the sequence $(F(\boldsymbol{x}_{n_k}))$ converges with the required rate of convergence for (i) of Lemma 3.1. The sequence $(\boldsymbol{x}_{n_k}, F(\boldsymbol{x}_{n_k}))$ then satisfies (i)–(iii) of Lemma 3.1, so the fact that $N(\boldsymbol{x}_{n_k}, F(\boldsymbol{x}_{n_k}))$ holds for each k implies, by Lemma 3.1(iv)(b), that $N(\boldsymbol{x}, \boldsymbol{y})$ holds, where $\boldsymbol{y} = \lim_{k\to\infty} F(\boldsymbol{x}_{n_k})$.

The argument is complicated by the fact that the $\boldsymbol{x}_k$ need not all lie in one cell. Instead of a single function F, we use Proposition 2.10 repeatedly to construct a sequence (F_k) of functions whose graphs lie in cells where G holds. If $\boldsymbol{x}_k$ and $\boldsymbol{x}_{k+1}$ lie in the same cell, then $F_k = F_{k+1}$. When $\boldsymbol{x}_k$ jumps to a new cell, the function F_k changes, but in such a way that $|F_k(\boldsymbol{x}_k) - F_{k+1}(\boldsymbol{x}_{k+1})|$ remains small. (For the p-adics, 'small' means 'less than p^{-k}'.) The fact that $G(\boldsymbol{x}_k, F_k(\boldsymbol{x}_k))$ holds ensures that this can be done. This method produces a sequence $(\boldsymbol{x}_k, F_k(\boldsymbol{x}_k))$ satisfying (i)–(iii) of Lemma 3.1, so as before, $N(\boldsymbol{x}, \boldsymbol{y})$ holds in the limit. □

Theorem 3.4 establishes a condition for sentences built from simple formulae to be constructively valid. The scope of Theorem 3.4 can be extended by showing that the class of formulae equivalent over $\mathbb{Q}_p$ to simple formulae is closed under

certain operations. This is done by using Theorem 3.4 to prove a stronger version of Lemma 3.1(iv)(a). In describing classes of p-adic algebraic formulae, a condition '$P_N(x)$' is called a *weak* Nth power condition and '$\tilde{P}_N(x)$' is called a *strict* Nth power condition. Two classes of formulae are distinguished. $\mathscr{F}_1$ is the class of all formulae equivalent over $\mathbb{Q}_p$ to simple formulae, and $\mathscr{F}_2$ is the class of all formulae equivalent over $\mathbb{Q}_p$ to conjunctions of disjunctions of strict nth power conditions.

Corollary 3.5. *$\mathscr{F}_2$ contains the strict Nth power formulae, and is closed under &, $\vee$ and $\exists$ relativised to a formula in $\mathscr{F}_1$. $\mathscr{F}_1$ contains identities, weak Nth power formulae and all members of $\mathscr{F}_2$, and is closed under &, $\forall$ relativised to a formula in $\mathscr{F}_1$, and the formation of conditionals with antecedents in $\mathscr{F}_2$.*

Proof. Using similar methods to those in the proof of Lemma 3.1(iv), the proof of the corresponding result in the reals [19, Corollary 1] can be adapted to prove this result. □

4. The intuitionistic theorem

We now want to consider the status of simple formulae $M(\boldsymbol{x})$ and $N(\boldsymbol{x}, \boldsymbol{y})$ for which the sentence $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$ fails over Q_p. A converse to Theorem 3.4 would say that, in this case, $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \rightarrow \exists \boldsymbol{y}\, N(\boldsymbol{x}, y))$ fails to hold over $\mathbb{Q}_p$. That this implication does not hold classically can be seen in an example where there is no condition M, and N defines the closure of the graph of the function taking $x \neq 0$ to its nth power coset representative. The second implication above holds classically, but points (x, y) obeying N need not vary continuously with x, so the first does not. This section uses principles of intuitionism to prove an intuitionistic converse to Theorem 3.4.

Brouwer's principle for numbers [12] states that, if $A \subseteq ({}^{\omega}\omega) \times \omega$ and

$$\forall p \in {}^{\omega}\omega\, \exists k\, ((p, k) \in A),$$

then there is a continuous function $h : {}^{\omega}\omega \rightarrow \omega$ such that

$$\forall p \in {}^{\omega}\omega\, ((p, h(p)) \in A).$$

The principle is not as strong as Brouwer's principle for functions, but Scowcroft [19] has shown that restricted versions of the principle for functions can be derived from the principle for numbers, as in the following lemma.

Lemma 4.1 (Scowcroft [19, Lemma 3]). *Assume Brouwer's principle for numbers. If $A \subseteq ({}^{\omega}\omega)^2$ is closed and*

$$\forall p \in {}^{\omega}\omega\, \exists q \in {}^{\omega}\omega\, ((p, q) \in A),$$

then there is a continuous function $h: {}^{\omega}\omega \to {}^{\omega}\omega$ *such that*

$$\forall p \in {}^{\omega}\omega\ ((p, h(p)) \in A).$$

The following notation is useful. If $S(\boldsymbol{x})$ is a p-adic algebraic formula, $\mathscr{S}^* = \{\boldsymbol{x} \in \mathbb{Q}_p^m : S(\boldsymbol{x})\}$ and $\mathscr{S} = \mathscr{S}^* \cap Q_p^m$. For any $\boldsymbol{x} \in Q_p^m$ and $r \in Q_p^*$, $B(\boldsymbol{x}, r) = \{\boldsymbol{u} \in \mathbb{Q}_p^n : |\boldsymbol{x} - \boldsymbol{u}| < |r|\}$ and $B_{Q_p}(\boldsymbol{x}, r) = B(\boldsymbol{x}, r) \cap Q_p^m$.

Suppose that $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \to \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$ holds over $\mathbb{Q}_p$. In order to prove an intuitionistic converse to Theorem 3.4, we want to show that $\forall \boldsymbol{x}\,(M(\boldsymbol{x}) \to \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$ holds over Q_p. Recall the definition of $G(\boldsymbol{x}, \boldsymbol{y})$ from Lemma 3.2. Given a c.a.d. of Q_p^{m+n}, let $\boldsymbol{x}$ be an element of a cell C_σ of the induced c.a.d. of Q_p^m such that $M(\boldsymbol{x})$ holds. In order to show $\exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y})$, we have to be able to say something about the sets $\mathscr{M}^* \cap B(\boldsymbol{x}, r)$ for every r such that $B(\boldsymbol{x}, r)$ is contained in the union of C_σ with the cells of higher rank. Furthermore, we want to relate these sets to ${}^{\omega}\omega$ in order to apply the intuitionistic result of Lemma 4.1. These are both done in Lemma 4.2.

Lemma 4.2. *Let* $M(x_1, \ldots, x_m)$ *be a simple formula,* $\mathscr{C}$ *a c.a.d. of* Q_p^m *invariant with respect to the terms and nth power conditions appearing in* M, *and* C_σ *a cell of* $\mathscr{C}$ *contained in* $\mathscr{M}$. *If* $\boldsymbol{x} \in C_\sigma$, $r \in Q_p^*$ *and* $B_{Q_p}(\boldsymbol{x}, r)$ *is contained in the union of* C_σ *with the cells of higher rank, then there is a continuous, surjective, relatively open map*

$$F: {}^{\omega}\omega \to \mathscr{M}^* \cap B(\boldsymbol{x}, r),$$

where 'relatively open' means that F maps open subsets of ${}^{\omega}\omega$ *onto subsets of* $\mathbb{Q}_p^m$ *which are open in* $\mathscr{M}^*$.

Proof. The proof follows the same general outline as the proof of the corresponding result for the reals [19, Lemma 4]. The following outline of the proof mentions the changes which need to be made to adapt to the p-adic topology. F is constructed by downward induction on the rank of the cell C_σ containing $\boldsymbol{x}$, and F is given as the limit of a function φ mapping sequences from ${}^{<\omega}\omega \to Q_p^m$. φ is defined so that the sequences $(\varphi(t \restriction n))_n$ satisfy properties (i)–(iii) of Lemma 3.1. Hence, if F is defined by $F(t) = \lim_{n\to\infty} \varphi(t \restriction n)$ for every $t \in {}^{\omega}\omega$, F is well-defined and continuous, and if $\varphi(t \restriction n) \in \mathscr{M}$ for every n, then also $F(t) \in \mathscr{M}^*$. Thus the substance of the proof is in the definition of φ. In fact, for every integer k we construct a φ which satisfies the stronger convergence property $|\varphi(\gamma) - \varphi(\gamma^\frown \delta)| < p^{-(k+\mathrm{lh}(\delta))}$ for every $\gamma, \delta \in {}^{<\omega}\omega$.

Let $d = \dim(C_\sigma)$. By Proposition 2.9(i), there is a continuous, continuously invertible function π_σ mapping C_σ and $C_\sigma \cap B_{Q_p}(\boldsymbol{x}, r)$ to open subsets of Q_p^d. Using the fact that continuous functions are uniformly continuous on compact subsets of their domains (Proposition 2.14) we can form the collection A of closed balls in $\pi_\sigma(C_\sigma \cap B_{Q_p}(\boldsymbol{x}, r))$ whose inverse images under π_σ have diameter less than p^{-k}. Let $b: \omega \twoheadrightarrow A$ enumerate A and define chains l of balls in A inductively.

$l(\langle i \rangle) = b(i)$ and given $l(\tau)$, let $b_\tau : \omega \to A$ enumerate those members of A contained in the interior of $l(\tau)$ whose inverse images under π_σ have diameter less than $p^{-(k+\mathrm{lh}(\tau))}$. Then $l(\tau^\frown i) = b_\tau(i)$. Although a p-adic ball does not have a uniquely defined center, we can define functions $c : {}^{<\omega}\omega \to Q_p^d$ and $p : {}^{<\omega}\omega \to Q_p$ to satisfy $l(\tau) = B_{Q_p}(c(\tau), \rho(\tau))$. The points $y_\tau = (\pi_\sigma \restriction C_\sigma)^{-1} c(\tau)$ satisfy $|y_\gamma - y_{\gamma^\frown\delta}| < p^{-(k+\mathrm{lh}(\tau))}$, and the inverse image of $l(\tau)$ under π_σ is contained in the intersection of C_σ with $B_{Q_p}(\boldsymbol{x}, r)$ and $B_{Q_p}(y_\tau, p^{k+\mathrm{lh}(\tau)})$. We can now define $\varphi(\tau)$. If every entry of τ is even — $\tau = 2 \cdot \delta$ — then $\varphi(\tau) = y_\delta$. If τ has some odd entry — $\tau = (2 \cdot \delta)^\frown(2i+1)^\frown\gamma$ — then $\varphi(\tau) = y_{\delta^\frown(2i+1)^\frown\gamma}$, unless the ball $B_{Q_p}(y_\tau, p^{k+\mathrm{lh}(\tau)})$ contains points in a cell of higher rank than $\mathrm{rk}(C_\sigma)$ which lie in $\mathcal{M} \cap B_{Q_p}(\boldsymbol{x}, r)$. In this case, the value of $\varphi(\tau)$ is given by a function defined at an earlier stage of the induction. This alternation of cases ensures that F will be onto $\mathcal{M}^* \cap B(\boldsymbol{x}, r)$.

To show that F is surjective and relatively open is fairly lengthy. Given a point $z \in \mathcal{M}^* \cap B(\boldsymbol{x}, r)$, let (z_n) be a sequence in $\mathcal{M}$ given by Lemma 3.1; we can assume the sequence is in $B_{Q_p}(\boldsymbol{x}, r)$. If the first term of the sequence is not in C_σ then, by (ii) and (iii) of Lemma 3.1, the sequence is bounded away from C_σ and the properties of the function defined at an earlier stage of the induction on $\mathrm{rk}(\sigma)$ can be invoked to show that $z \in \mathrm{ran}(F)$. If the first term of the sequence is in C_σ, then we use an inductive procedure to construct a sequence $q \in {}^\omega\omega$ such that $\lim_{n\to\infty} \varphi(q \restriction n) = \lim_{n\to\infty, z_n \in C_\sigma} z_n$. This serves as the basis of an inductive procedure to construct $t \in {}^\omega\omega$ such that $F(t) = z$. Similar constructions establish that the images of open sets in ${}^\omega\omega$ under F are relatively open sets in $\mathcal{M}^*$. □

One can now prove Theorem 4.3, using Lemmas 4.1 and 4.2, and the results of Section 3. Let $M(x_1, \ldots, x_m)$ and $N(x_1, \ldots, x_m, y_1, \ldots, y_n)$ be simple formulae, and $G(\boldsymbol{x}, \boldsymbol{y})$ the formula generated from M and N in Lemma 3.2.

Theorem 4.3. *Assume Brouwer's principle for numbers. If*

$$\forall \boldsymbol{x}\, (M(\boldsymbol{x}) \to \exists \boldsymbol{y}\, N(\boldsymbol{x}, \boldsymbol{y}))$$

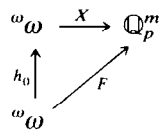
holds over $\mathbb{Q}_p$, *then*

$$\forall \boldsymbol{x}\, (M(\boldsymbol{x}) \to \exists \boldsymbol{y}\, G(\boldsymbol{x}, \boldsymbol{y}))$$

holds over Q_p.

Proof. Once again, only an outline of the proof will be given. To start the proof, notice that we are only interested in G over Q_p. Since every p-adic formula is equivalent over Q_p to a simple formula, we can assume that G is a simple formula. By Lemma 3.2 there is a c.a.d. $\mathcal{C}$ of Q_p^{m+n} which is invariant with respect to the terms and rth power conditions appearing in M, N and G, and with respect to which G has the continuity property.

We can define two different continuous functions from ${}^{\omega}\omega$ into $\mathbb{Q}_p^m$. On the one hand, given $\boldsymbol{x} \in \mathcal{M}$, Lemma 4.2 provides a continuous, relatively open function F from ${}^{\omega}\omega$ onto $B(\boldsymbol{x}, \varepsilon) \cap \mathcal{M}^*$ where ε is chosen so that $B_{Q_p}(\boldsymbol{x}, \varepsilon)$ is contained in the union of $\boldsymbol{x}$'s cell (in the c.a.d. of Q_p^m induced by $\mathcal{C}$) with the cells of higher rank. On the other hand, consider all finite sequences $\langle(\boldsymbol{x}_1, \boldsymbol{y}_1), \ldots, (\boldsymbol{x}_k, \boldsymbol{y}_k)\rangle$, with $\boldsymbol{x}_i \in \mathcal{M}$ and $(\boldsymbol{x}_i, \boldsymbol{y}_i) \in \mathcal{N}$, which satisfy properties (i)–(iii) of Lemma 3.1. By enumerating these sequences and taking limits, one can define functions $(X, Y): {}^{\omega}\omega \to \mathbb{Q}_p^{m+n}$. Properties (i)–(iii) ensure that X and Y are well-defined and continuous, while the rest of Lemma 3.1 ensures that $(X(s), Y(s)) \in \mathcal{N}^*$ for every $s \in {}^{\omega}\omega$ and that X maps onto $\mathcal{M}^*$. Thus, for every $p \in {}^{\omega}\omega$ there is $q \in {}^{\omega}\omega$ such that $F(p) = X(q)$. Brouwer's principle for numbers and Lemma 4.1 provide a continuous function $h_0: {}^{\omega}\omega \to {}^{\omega}\omega$ so that the diagram



commutes.

Fix $p \in {}^{\omega}\omega$ such that $\boldsymbol{x} = F(p) = Xh_0(p)$. The problem is to find a $\boldsymbol{y} \in Q_p^n$ such that $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{G}$. By definition of X and Y, $(Xh_0(p), Yh_0(p))$ is given by a sequence $(\boldsymbol{x}_k, \boldsymbol{y}_k)$ satisfying properties (i)–(iii) of Lemma 3.1. If this sequence lies in $\mathcal{G}$, then the limit is also in $\mathcal{G}^*$, by Lemma 3.1(iv)(b). This is not quite enough, however, as $Yh_0(p) \in \mathbb{Q}_p^n$ but not necessarily in Q_p^n. But if the sequence $(\boldsymbol{x}_k)$ is constant and $(\boldsymbol{x}_k, \boldsymbol{y}_k) \in \mathcal{G}$ for each k, then this says exactly that $(Xh_0(p), \boldsymbol{y}_k) \in \mathcal{G}$ for each k. Since $Xh_0(p) \in Q_p^m$, this situation can be forced by refining the c.a.d. $\mathcal{C}$ to a c.a.d. with $\{Xh_0(p)\}$ as a cell. Property (ii) of Lemma 3.1 then requires that eventually the sequence $(\boldsymbol{x}_k)$ is constant.

The only problem remaining is to show that a subsequence of $(\boldsymbol{x}, \boldsymbol{y}_k)$ can be chosen to lie in $\mathcal{G}$. This is done by an inductive procedure. If $(\boldsymbol{x}, \boldsymbol{y}_k) \notin \mathcal{G}$ for some k, one can use the fact that F is relatively open (recalling that $\boldsymbol{x} = F(p)$) to find an integer $n > k$ at which the sequence changes cell to a cell of higher rank. Since there are only finitely many cells, eventually the sequence lies in $\mathcal{G}$. □

In [19], Scowcroft discusses how one can weaken the hypothesis of his Theorem 2, the analogue to my Theorem 4.3. The version of the principle for functions from Lemma 4.1 implicitly allows the use of choice-sequence parameters in the predicate defining A. In both the reals and the p-adics, the lemma is applied to predicates of the form $F(s) = X(t)$, where F and X are continuous functions, definable in second-order arithmetic, whose definitions do not use extra choice-sequence parameters. Scowcroft shows [19, Lemma 5] that this weaker corollary to Lemma 4.1 can be established using a weaker form of Brouwer's principle for numbers, monotone bar induction and relativised dependent choice. As a result, one can obtain the conclusion of Theorem 3.4 with these weaker hypotheses.

Appendix

This section contains the proof of Theorem 2.11. For convenience, the theorem is stated again here.

Theorem 2.11. *Let $f: U \to Q_p$ be a bounded, definable function whose domain includes a punctured open ball $U \subset Q_p$ around the origin. One can find an open set $A \subseteq U$ with $0 \in \mathrm{cl}(A)$ such that $\lim_{x \to 0, x \in A} f(x)$ exists in Q_p.*

Proof. Since f is a definable function, there is a polynomial $g(X, Y)$ such that, for every $x \in U$, $g(x, f(x)) = 0$. As noted in the proof of Theorem 2.8, Q_p is a factorial field, so by [14, Theorem IV.4.9], $Q_p[X]$ is also factorial. Thus we can write $g(x, Y) = g_1(X, Y) \cdots g_r(X, Y)$ as a product of irreducible polynomials in $Q_p[X, Y]$. As in the discussion of Theorem 2.8, there is a discrete algebraic closure Q_p^{alg} of Q_p. Over Q_p^{alg}, the procedure of [21, IV, §3] gives an algorithm for computing the roots of the $g_i(X, Y)$ as formal Laurent series in fractional powers of X:

$$g_i(X, Y) = g_{in_i}(X) \prod_{i=1}^{n_i} (Y - \alpha_{ij}(X)), \qquad \alpha_{ij}(X) \in \bigcup_{s=1}^{\infty} Q_p^{\mathrm{alg}}((X^{1/s})).$$

(Walker's argument is nonconstructive only at the point where he confirms that there is a finite bound on the size of the denominators which appear in the fractional powers. For irreducible polynomials, this point can be made constructive using the comment in [21, p. 105 (Dover edition)] and properties of the discriminant.) One can choose a sufficiently large denominator s, such that each $\alpha_{ij}(X)$ can be written as $\alpha_{ij}(X) = \sum_{l=M_{ij}}^{\infty} \alpha_{ijl} X^{l/s}$, where $M_{ij} \in \mathbb{Z}$. For each $1 \leq i \leq r$, let $G_i = \{x \in U: g_i(x, f(x)) = 0 \ \& \ \tilde{P}_s(x)\}$. The G_i are definable sets and $\bigcup_{i=1}^{r} G_i = \{x \in U: \tilde{P}_s(x)\}$. Hence there is $1 \leq i_0 \leq r$ such that G_{i_0} has nonempty interior [20, Lemma 1.2] and $0 \in \mathrm{cl}(G_{i_0})$. Take V to be an open definable subset of G_{i_0} with $0 \in \mathrm{cl}(V)$ and let $g_{i_0}(X, Y) = q(X, Y)$. Then, adapting the notation so that $q_n(X) = g_{in_i}(X)$ and so on, $q(X, Y) = q_n(X) \prod_{i=1}^{n} (Y - \alpha_i(X))$,

$$\alpha_i(X^s) = \sum_{i=M_i}^{\infty} \alpha_{il} X^l$$

and for any $x \in V$, $q(x, f(x)) = 0$. Since $q_n(X)$ has only isolated zeros, we can assume that $q_n(x) \neq 0$ for $x \in V$. Consider $q(X, Y)$ as a polynomial over $Q_p^{\mathrm{alg}}(X)$, which is a discrete subfield of the ring $Q_p^{\mathrm{alg}}((X^{1/s}))$. The roots $\alpha_1(X), \ldots, \alpha_n(X)$ are algebraic over $Q_p^{\mathrm{alg}}(X)$, and it is straightforward to show that $Q_p^{\mathrm{alg}}((X^{1/s}))$ satisfies the hypotheses of [14, Theorem VI.1.9], and hence $Q_p^{\mathrm{alg}}(X)[\alpha_1(X), \ldots, \alpha_n(X)]$ is discrete. As $q(X, Y)$ is irreducible, the roots $\alpha_i(X)$ are apart in $Q_p^{\mathrm{alg}}(X)[\alpha_1(X), \ldots, \alpha_n(X)]$. Since the apartness relation is given by comparing coefficients, this means that one can find a nonnegative integer N such that, for every $1 \leq i \neq j \leq n$, there is $l \leq N$ with $\alpha_{il} \neq \alpha_{jl}$.

Let $h(x)=f(x^s)$ and $\beta_i(X)=\alpha_i(X^s)$ for each $1\leq i\leq n$. So $q(X^s, Y)=q^n(X^s)\prod_{i=1}^n(Y-\beta_i(X))$ and $q(x^s, h(x))=0$ for every x with $x\in W=\{x: x^s\in V\}$. If one can find an open definable set $B\subseteq W$ with $0\in \mathrm{cl}(B)$ such that $\lim_{x\to 0, x\in B} h(x)$ exists in Q_p, this is enough to prove the theorem; for if

$$A=\{z\in Q_p: \exists x\in B\,(x^s=z)\},$$

then

$$\lim_{z\to 0,\, z\in A} f(z)=\lim_{x\to 0, x\in B} h(x)\in Q_p.$$

One only needs to check that A is open and $0\in \mathrm{cl}(A)$. A is the inverse image of B under all branches of the function which takes a number to an sth root. Since the number of sth roots of any nonzero sth power x is constant and independent of x (a simple corollary to [15, Lemma 2.5]), one can use [20, Theorem 1.1] to show that every branch of the sth root function is continuous away from 0. Hence, since B is open and $0\in \mathrm{cl}(B)$, also A is open and $0\in \mathrm{cl}(A)$.

Thus, it remains to find B. The idea is to have $h(x)=\beta_i(x)$ for some i and every x in B. For then, $\lim_{x\to 0, x\in B} h(x)=\lim_{x\to 0, x\in B}\beta_i(x)$. We must first ensure that the β_i which is chosen has a well-defined limit at 0, and that the limit is in Q_p. Using the valuation on Q_p^{alg} described in the discussion of Theorem 2.8, one can form the completion $\tilde{Q}_p$ of Q_p^{alg} as in [2]. An argument similar to that in [7, XXX, §18] shows that each $\beta_i(x)$ is convergent (in $\tilde{Q}_p$) in a punctured neighbourhood of 0. Taking the smallest of these neighbourhoods, one can say that $\beta_i(x)$ is convergent for $1\leq i\leq n$ if $0<|x|<|\delta_1|$ and $x\in W$. Since $f(x)$ is bounded on V and therefore also $h(x)$ is bounded on W, there is $K\in Q_p^*$ such that $|h(x)|<|K|$ for $0<|x|<|\delta_1|$. If $M_i<0$ for some $1\leq i\leq n$, then $|\beta_i(x)|=|\alpha_{iM_i}x^{M_i}|\geq|K|$ for sufficiently small nonzero x in Q_p. Hence $h(x)\neq\beta_i(x)$ if $0<|x|<|\delta_2|<|\delta_1|$, so one can omit for consideration those $\beta_i(X)$ for which $M_i<0$. Similarly, if $\alpha_{il}\notin Q_p$ for some i and $0\leq l\leq N$, then, as in the discussion of Theorem 2.8, $|\alpha_{il}-\gamma|>p^{-t}$ for some integer t and every $\gamma\in Q_p$. If l is the first integer with $\alpha_{il}\notin Q_p$, then

$$\beta_i(X)=\sum_{k=0}^{i-1}\alpha_{ik}X^k+X^l\Big(\alpha_{il}+\sum_{k=l+1}^{\infty}\alpha_{ik}X^{k-l}\Big).$$

For sufficiently small nonzero x in Q_p, $|\sum_{k=l+1}^{\infty}\alpha_{ik}x^{k-l}|<p^{-t}$, so $x^l(x_{il}+\sum_{k=l+1}^{\infty}\alpha_{ik}x^{k-l})$ is not in Q_p. Since $\sum_{k=0}^{l-1}\alpha_{ik}x^k\in Q_p$, $\beta_i(x)\notin Q_p$. Hence, for $0<|x|<|\delta_3|<|\delta_2|$, $h(x)\neq\beta_i(x)$ if $\alpha_{il}\notin Q_p$ for any $1\leq l\leq N$, and one can omit these roots from consideration. Relabel so that the remainder are $\{\beta_i(x)\}_{i=1}^r$.

Now we would like to say that, since $W=\bigcup_{i=1}^r\{x: h(x)=\beta_i(x)\}$ is open, one of the sets in this union must itself be open and can be taken for B. However, this is not obviously a union of definable sets, so we must proceed more carefully. The polynomials $\sum_{l=0}^N(\alpha_{il}-\alpha_{jl})x^l$ for $1\leq i<j\leq r$ are all nonzero by the choice of N,

so one can find $\varepsilon \in Q_p^*$ and $\delta_4 \in Q_p^*$ such that

$$\left|\sum_{l=0}^{N} (\alpha_{il} - \alpha_{jl})x^N\right| \geqslant |\varepsilon|\,|x^N| \tag{4}$$

on $\{x \in W: 0 < |x| < |\delta_4|\}$. Without loss of generality one can assume that $|\delta_4| < |\delta_3|$ and so

$$\left|\beta_i(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right| = \left|\sum_{l=N+1}^{\infty} \alpha_{il}x^l\right| = |x^N|\left|\sum_{l=1}^{\infty} \alpha_{i(l+N)}x^l\right|$$

on $\{x \in W: 0 < |x| < |\delta_4|\}$. $\sum_{l=1}^{\infty} \alpha_{i(l+N)}x^l$ is convergent on this set, and is zero when $x = 0$, so one can find $0 \neq |\delta_5| < |\delta_4|$ such that

$$\left|\beta_i(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right| < |\varepsilon|\,|x^N| \tag{5}$$

on $\{x \in W: 0 < |x| < |\delta_5\}$ for every $1 \leqslant i \leqslant r$. Define

$$B_i = \left\{x \in W: 0 < |x| < |\delta_5| \;\&\; \left|h(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right| < |\varepsilon|\,|x^N|\right\},$$

for $1 \leqslant i \leqslant r$. If $x \in B_i$, then $h(x) = \beta_i(x)$; for if $|h(x) - \beta_j(x)| < |\varepsilon|\,|x^N|$ for some $j \neq i$, then

$$\left|h(x) - \sum_{l=0}^{N} \alpha_{jl}x^l\right| \leqslant \max\left\{|h(x) - \beta_j(x)|, \left|\beta_j(x) - \sum_{l=0}^{N} \alpha_{jl}x^l\right|\right\} < |\varepsilon|\,|x^N|$$

by (5). Hence

$$\begin{aligned}\left|h(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right| &= \max\left\{\left|h(x) - \sum_{l=0}^{N} \alpha_{jl}x^l\right|, \left|\sum_{l=0}^{N} \alpha_{jl}x^l - \sum_{l=0}^{N} \alpha_{il}x^l\right|\right\} \\ &\geqslant |\varepsilon|\,|x^N| \quad \text{by (4)},\end{aligned}$$

which contradicts $x \in B_i$. Thus $|h(x) - \beta_j(x)| > 0$ for any $j \neq i$, so $h(x) \neq \beta_j(x)$. Since $q(x^s, h(x)) = 0$, it must be the case that $h(x) = \beta_i(x)$. Thus for any $1 \leqslant i \leqslant r$,

$$\lim_{x \to 0, x \in B_i} h(x) = \lim_{x \to 0, x \in B_i} \beta_i(x) = \beta_i(0) \in Q_p. \tag{6}$$

To finish the proof, notice that $q_n(x^s)\prod_{i=1}^{r}(h(x) - \beta_i(x)) = 0$ and $q_n(x^s) \neq 0$ for every $x \in W$, so for at least one $1 \leqslant i \leqslant r$, $|h(x) - \beta_i(x)| < |\varepsilon|\,|x^N|$. Thus

$$\left|h(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right| \leqslant \max\left\{|h(x) - \beta_i(x)|, \left|\beta_i(x) - \sum_{l=0}^{N} \alpha_{il}x^l\right|\right\} < |\varepsilon|\,|x^N|$$

if $|x| < |\delta_5|$. Hence $\bigcup_{i=1}^{r} B_i = \{x \in W: 0 < |x| < |\delta_5|\}$, which is open. Since the B_i are open definable sets, at least one of them, say B, has nonempty interior and 0 as a limit point. This B is as required. □

Acknowledgement

I would like to thank Philip Scowcroft for his advice concerning this extension of his work to the p-adics.

References

[1] M. Beeson, Foundations of Constructive Mathematics, Ergeb. Math. Grenzgeb. (3) 6 (Springer, Würzburg, 1985).
[2] E. Bishop and D. Bridges, Constructive Analysis, Grundlehren Math. Wiss. 279 (Springer, Berlin, 1985).
[3] D. Bridges and F. Richman, Varieties of Constructive Mathematics, London Math. Soc. Lecture Notes Ser. 97 (Cambridge Univ. Press, Cambridge, 1987).
[4] L. Bröcker and J.-H. Schinke, On the L-adic Spectrum, Schriftenreihe Math. Inst. Univ. Münster, Ser. 2, 40 (Univ. Münster, Münster, 1986).
[5] L.E.J. Brouwer, Points and spaces, in: A. Heyting, ed., Collected Works, Vol. 1, Philosophy and Foundations of Mathematics (North-Holland, Amsterdam, 1975) 522–538, also: Canad. J. Math. 6 (1954) 1–17.
[6] J.W.S. Cassels, Local Fields, London Math. Soc. Stud. Texts 3 (Cambridge Univ. Press, Cambridge, 1986).
[7] G. Chrystal, Algebra, Vols. 1 and 2 (Chelsea, New York, 7th ed., 1964).
[8] G. Collins, Quantifier elimination for real closed fields by cylindrical algebraic decomposition, in: H. Brakhage, ed., Automata Theory and Formal Languages: 2nd G.I. Conference, Lecture Notes in Comput. Sci. 33 (Springer, Berlin, 1975) 134–183.
[9] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. 77 (1984) 1–23.
[10] J. Denef, p-adic semi-algebraic sets and cell decomposition, J. Reine Angew. Math. 369 (1986) 154–166.
[11] D. Haskell, Topics in constructive p-adic algebra, Ph.D. Thesis, Stanford Univ. 1990.
[12] S.C. Kleene and R.E. Vesley, The Foundations of Intuitionistic Mathematics, Stud. Logic Found. Math. (North-Holland, Amsterdam, 1965).
[13] A. Macintyre, On definable subsets of p-adic fields, J. Symbolic Logic 41 (1976) 605–610.
[14] R. Mines, F. Richman and W. Ruitenburg, A Course in Constructive Algebra, Universitext (Springer, New Jersey, 1988).
[15] E. Robinson, Geometric theory of p-adic fields, J. Algebra 110 (1987) 158–172.
[16] P. Scowcroft, The real-algebraic structure of Scott's model of intuitionistic analysis, Ann. Pure Appl. Logic 27 (3) (1984) 275–308.
[17] P. Scowcroft, More on real algebra in Scott's model, Ann. Pure Appl. Logic 30 (3) (1986) 277–291.
[18] P. Scowcroft, A note on definable Skolem functions, J. Symbolic Logic 53 (1988) 905–911.
[19] P. Scowcroft, A transfer theorem in constructive real algebra, Ann. Pure Appl. Logic 40 (1) (1988) 29–87.
[20] P. Scowcroft and L. van den Dries, On the structure of semi-algebraic sets over p-adic fields, J. Symbolic Logic 53 (1988) 1138–1164.
[21] R.J. Walker, Algebraic Curves (Princeton Univ. Press, Princeton, NJ, 1950); reprinted: (Dover, New York, 1962).